TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

ANALÝZA RIZIK CAR-TO-X KOMUNIKACE

Bakalářská práce

Studijní program: B2612 – Elektrotechnika a informatika
Studijní obor: 1802R022 – Informatika a logistika

Autor práce: **Dominik Spiral**
Vedoucí práce: Ing. Jan Kamenický Ph.D.

Liberec 2017

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Mechatronics, Informatics
and Interdisciplinary Studies

RISK ANALYSIS OF CAR-TO-X COMMUNICATION

Bachelor Thesis

Study Programme:	B2612 – Electrical Engineering and Informatics
Study Branch:	1802R022 – Informatics and Logistics
Author:	**Dominik Spiral**
Supervisor:	Ing. Jan Kamenický Ph.D.

Liberec 2017

Technická univerzita v Liberci
Fakulta mechatroniky, informatiky a mezioborových studií
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Dominik Spiral**
Osobní číslo:	**M15000226**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Informatika a logistika**
Název tématu:	**Analýza rizik Car-to-X komunikace**
Zadávající katedra:	**Ústav mechatroniky a technické informatiky**

Zásady pro vypracování:

1. Popište technické vlastnosti technologií, používaných pro bezdrátový přenos dat v rámci Car-to-X komunikace v automobilovém průmyslu.
2. Popište rizika všech typů Car-to-X komunikací.
3. Proveďte analýzu FMECA jednotlivých typů komunikací Car-to-X. Porovnejte jednotlivá identifikovaná rizika.
4. Navrhněte opatření pro minimalizaci rizik.
5. Diskutujte potenciální přínosy a náklady navržených opatření.

Rozsah grafických prací: **dle potřeby dokumentace**

Rozsah pracovní zprávy: **30–40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] **HAGEN STÜBING. Multilayered Security and Privacy Protection in Car-to-X Networks Solutions from Application down to Physical Layer. Wiesbaden: Springer Fachmedien Wiesbaden, 2013. ISBN 9783658025304.**

[2] **GUPTA, Naresh C. Inside Bluetooth low energy. Boston: Artech House, 2013. Artech House mobile communications series. ISBN 978-1-60807-580-5.**

Vedoucí bakalářské práce: **Ing. Jan Kamenický, Ph.D.**
Ústav mechatroniky a technické informatiky

Konzultant bakalářské práce: **Ing. Pavel Novák**
Škoda Auto, a.s.

Datum zadání bakalářské práce: **10. října 2016**

Termín odevzdání bakalářské práce: **15. května 2017**

prof. Ing. Zdeněk Plíva, Ph.D.
děkan

Technická univerzita v Liberci
L.S.
14

doc. Ing. Milan Kolář, CSc.
vedoucí ústavu

V Liberci dne 10. října 2016

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum: 11. 05. 2017

Podpis:

Poděkování

Tímto děkuji panu Ing. Janu Kamenickému, Ph.D. za vedení mé bakalářské práce, ochotu a cenné rady, které mi pomohly ji zkompletovat. Také děkuji panu Ing. Pavlu Novákovi za konzultaci práce.

Abstrakt

Tato bakalářská práce se zabývá analýzou rizik spjatých s implementací technologie Car-to-X, která umožňuje komunikaci mezi vozy a dopravní infrastrukturou na bázi bezdrátových radiofrekvenčních technologií IEEE 802.11 a LTE. K řešení je použita spolehlivostní metoda analýzy způsobů, důsledků a kritičnosti poruch FMECA. V rámci analýzy jsou k identifikovaným problémům navrhnuta opatření umožňující jejich odstranění či minimalizaci. Výsledky této analýzy mohou napomáhat bezpečnému uvedení technologií Car-to-X do reálného provozu.

Klíčová slova: Car-to-X, bezdrátová komunikace, 802.11p, LTE, FMECA

Abstract

This bachelor's thesis deals with the analysis of risks associated with the implementation of Car-to-X technology which allows for communication between vehicles and the infrastructure based on IEEE 802.11 and LTE wireless radio technologies. For this, Failure Mode, Effects and Criticality Analysis (FMECA) reliability method is used. Measures to eliminate or minimize the effects of the identified problems are proposed in the analysis. The results of this analysis could help to ensure safe introduction of Car-to-X technologies into full operation.

Key words: Car-to-X, Wireless communication, 802.11p, LTE, FMECA

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

3G – Third Generation

3GPP – Third Generation Partnership Project

AEC – Automotive Electronics Council

AP – Access Point

AU – Application Unit

BMW – Bayerische Motoren Werke

BPSK – Binary Phase-Shift Keying

BSS – Basic Service Set

C-ITS – China Intelligent Transport Systems Industry Alliance

C2C-CC – Car 2 Car Communication Consortium

C2C/V2V – Car to Car/Vehicle to Vehicle

C2I/V2I – Car to Infrastructure/Vehicle to Infrastructure

C2M/V2M – Car to Mobile

C2P – Car to Pedestrian

C2X/V2X – Car-to-X/Vehicle-to-X

CA – Certifikační autorita

CAM – Co-operative Awareness Message

CAN – Controller Area Network

CCH – Control Channel

CDMA – Code Division Multiple Access

CEN – Comité Européen de Normalisation

CITS – Cooperative Intelligent Transport Systems

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

DCF – Distributed Coordination Function

DENM – Decentralized Environmental Notification Message

DSRC – Dedicated Short Range Communication

DoS – Denial of Service

ECU – Electronic Control Unit

EDCA - Enhanced Distribution Channel Access

ETSI – European Telecommunications Standards Institute

EU – Evropská Únie

FCC – Federal Communications Commision

FMEA – Failure Mode and Effects Analysis

FMECA – Failure Mode, Effects and Criticality Analysis

GNSS – Global Navigation Satellite System

GSM – Global System for Mobile Communications

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

IMSI – International Mobile Subscriber Identity

IP – Internet Protocol

ITS – Intelligent Transport System

LTC – Long-Term Certificate

LTCA – Long-Term Certificate Authority

LTE – Long Term Evolution

LTE-A – Long Term Evolution Advanced

LTE-D2D – Long Term Evolution – Device to Device

LTE-V – Long Term Evolution Vehicular

MAC – Medium Access Control

MIMO – Multiple Input Multiple Output

MU-MIMO – Multi-User Multiple-Input Multiple-Output

NFC – Near Field Communication

OBU – On-Board Unit

OFDM – Orthogonal Frequency Division Multiplex

OFDMA – Orthogonal Frequency-Division Multiple Access

PC - Pseudonym Certificate

PCA – Pseudonym Certificate Authority

PHY – Physical layer

PKI – Public Key Infrastructure

QAM – Quadrature amplitude modulation

QPSK – Quadrature Phase-Shift Keying

RCA – Root Certificate Authority

RPN – Risk Priority Number

RSU – Road-Side Unit

SAE – Society of Automotive Engineers

SC-FDMA – Single-Carrier Frequency Division Multiple Access

SCH – Service Channel

SIM – Subscriber Identity Module

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

UMTS – Universal Mobile Telecommunications System

USA – United States of America

USDOT – United States Department of Transportation

V2Central – Vehicle to Central Infrastructure

V2Private – Vehicle to Private Network

V2R – Vehicle to Roadside

VIN – Vehicle Identification Number

WAVE – Wireless Access for Vehicular Environments

WSMP – WAVE Short Message Protocol

WiMAX – Worldwide Interoperability for Microwave Access

1 Úvod

Tématem bakalářské práce je analýza rizik, ke kterým může dojít během Car-to-X komunikace. Car-to-X je technologie, která představuje poslední etapu ve vývoji bezdrátové konektivity v automobilovém průmyslu. Konektivita jako celek tvoří jedno z nejrychleji se rozšiřujících témat automobilového vývoje. V minulosti sloužily bezdrátové technologie jako Bluetooth či Wi-Fi pouze pro propojení systému infotainment ve voze s uživatelskými zařízeními s cílem zvýšit komfort jízdy (Hands-Free technologie, přehrávání médií z telefonu atd.). V poslední době začaly být vozy také osazovány LTE modemy či využívat datového spojení mobilních telefonů. Připojení k internetové síti umožnilo přístup k online informacím o dopravě či nehodách. Poslední fází tohoto vývoje je technologie Car-to-X, která spočívá ve výměně informací vozu s ostatními vozy, prvky infrastruktury či jakoukoliv jinou vnější periferií umožňující bezdrátové spojení (např. směrovač v domácnosti, chytrý klíč atd.). Technologie Car-to-X přináší kromě zvýšení komfortu cestujících především výrazné zvýšení pasivní bezpečnosti provozu formou upozornění či automatizovanou reakcí na přijaté informace ze svého okolí. Informace, které vůz může prostřednictvím této technologie přijímat a vysílat v budoucnu umožní plnou automatizaci jeho řízení. S blížícím se nasazením takové technologie se ovšem pojí i velké množství bezpečnostních rizik, která je nutné adresovat, jelikož selhání takto komplexního systému řídícího veškerou dopravu může mít kritické následky.

Cílem bakalářské práce je provést rozbor a analýzu bezpečnostních rizik Car-to-X komunikace vozidla se svým okolím. Tato rizika jsou zkoumána pro každou bezdrátovou technologii, která se pro Car-to-X využívá. Důraz je v práci ovšem kladen na technologie založené na standardu IEEE 802.11, které mají v kontextu reálného nasazení Car-to-X největší relevanci. Pro vyhodnocení zjištěných rizik je použita metoda FMECA (analýza způsobů, důsledků a kritičnosti poruch). Vstupem pro analýzu jsou veškerá rizika, která byla u jednotlivých technologií, využívaných pro Car-to-X komunikaci, identifikována. Výstupem je návrh opatření pro minimalizaci zkoumaných rizik a zhodnocení jejich aplikovatelnosti s ohledem na náročnost a nákladnost.

V teoretické části práce jsou představeny principy a základní vlastnosti technologie Car-to-X. Navazující kapitola se věnuje popisu technických vlastností a parametrů jednotlivých bezdrátových technologií, které se v rámci Car-to-X pro přenos dat využívají. Konkrétně se jedná o rodinu standardů pro lokální bezdrátové sítě IEEE 802.11, zejména její dodatek pro bezdrátový přístup mezi vozy 802.11p, dále také standardy datových celulárních sítí Long Term Evolution (LTE). Kapitola čtvrtá tvoří praktickou část práce, ve které je na základě identifikace problémů spjatých s implementací technologie Car-to-X provedena spolehlivostní analýza metodou FMECA. Kapitola též obsahuje přípravnou část analýzy, včetně určení spolehlivostních faktorů a výsledné zhodnocení s diskuzí nad provedenou analýzou.

2 Principy Car-to-X komunikace

Car-to-X (zkráceně označováno jako C2X) je označení pro technologii, která umožňuje vozidlům a různým externím periferiím či prvkům infrastruktury (např. dopravnímu značení) komunikovat mezi sebou. Tato komunikace probíhá prostřednictvím zpráv, jejichž obsahem jsou například informace o stupni dopravy, nehodě či stavu vozovky. Každé vozidlo je jak příjemcem, tak odesílatelem těchto zpráv, vozy tak mezi sebou tvoří komplexní síť, ve které jsou si vědomy svých vzájemných poloh a okolní situace. Tyto informace jsou vozům k dispozici dříve, než je zaznamenají radarové systémy vozu či samotný řidič. S prvním sériovým nasazením budou sloužit pro včasné varování řidiče o možném nebezpečí mimo jeho dohled. V další generaci budou informace využity vozem pro asistované či plně autonomní řízení, jako doplněk radarů, čidel a kamer monitorujících bezprostřední okolí vozu (pro monitorování širšího okolí).

Implementace Car-to-X komunikace v širším měřítku by měla vést ke zvýšení jízdního komfortu pasažérů a zlepšení dopravní situace (např. vozidla budou na základě dostupných informací volit optimální trasy). Hlavní motivací pro její výzkum a vývoj s výhledem do budoucnosti je ovšem automatizace řízení a výrazné zvýšení bezpečnosti na silničních komunikacích.

2.1 Dělení Car-to-X komunikace

Technologie Car-to-X se dělí na několik základních podmnožin dle využití. Zde jsou vyjmenovány nejčastější z nich:

- **Car to Car (C2C)** – též často nazývaný Vehicle to Vehicle (V2V). Nejznámější způsob Car to X komunikace, který opisuje vzájemnou komunikaci mezi jednotlivými silničními vozy libovolného druhu (nákladní, osobní, atd.).
- **Car to Infrastructure (C2I)** – též Vehicle to Infrastructure (V2I). Jedná se o komunikaci vozidel se statickými prvky infrastruktury, jakými jsou například světelná signalizační zařízení či informační tabule na rychlostních komunikacích. Tento druh C2X komunikace se někdy dále dělí na *Vehicle to Roadside (V2R)* a *Vehicle to Central Infrastructure (V2Central)*. Další stupeň divize slouží pro rozlišení lokální komunikace s prvky v okolí vozidla a komunikace s dopravním

řídícím střediskem, která probíhá vzdáleně (za využití mobilní datové sítě). Většinou jsou ovšem pojmy *C2I* a *V2R* zaměnitelné, není-li také explicitně zmíněno V2Central. [1]

- **Car to Pedestrian (C2P)** – Komunikace mezi motorovými vozidly a chodci/cyklisty umožňující informování vozu o přesné poloze jedince na vozovce. V budoucnu by mohly být oboustranně komunikujícími C2P jednotkami osazeny například vozíčky, kočárky či jízdní kola. V současnosti se ovšem počítá s rozšířeným nasazením této technologie za využití chytrých mobilních zařízení, které u sebe nosí velké procento populace. [2]
- **Car to Home** – někdy také nazýváno Vehicle to Private Network (V2Private). [1] Tato kategorie C2X komunikace řeší všechny možnosti připojení vozidla k libovolné externí síti. V tomto kontextu se nemusí jednat pouze o domácí síť majitele vozu (prostřednictvím které se vůz připojuje k internetu za účelem získání softwarových či mapových aktualizací). Může se jednat například o spojení s indukční dobíjecí stanicí pro elektromobily (vzájemná výměna dat a identifikace) či spojení s drive through terminálem řetězce rychlého občerstvení.
- **Car to Mobile (C2M)** – také označováno jako V2M, někdy se takto označují současné možnosti propojení systému infotainment ve voze s mobilním zařízením za účelem poskytování komfortu a zábavy posádce (Bluetooth Hands Free atd.). V kontextu Car to X je ovšem relevantní komunikace telefonu s vozem v případech, kdy se zařízení ve voze nevyskytuje. V takových situacích může například sloužit jako klíč k vozu či pro jeho vzdálené parkování.
- **Car to Internet** – ne příliš často využívané označení pro přímé připojení vozidla do internetové sítě prostřednictvím 3G či LTE modemů, jimiž dnešní vozy disponují.

Rozdělení je pouze orientační, jelikož klasifikací existuje mnoho a zde jsou vyjmenovány pouze nejčastěji zmiňované. Velká variace spočívá ve faktu, že technologie je relativně nová a názvosloví stále není plně ustáleno. Car to Car, Car to Infrastructure a Car to Pedestrian (respektive jejich varianty se synonymem Vehicle) jsou pojmy standardizované hlavními světovými Car to X standardizačními organizacemi. Tyto tři

kategorie zabývající se bezpečností provozu lze zahrnout pod společný pojem CITS (Cooperative Intelligent Transport Systems). [4]

Ostatní kategorie, netýkající se bezpečnosti a plynulosti provozu, nemají přesně definované meze, tudíž se svým polem působnosti překrývají a různě nazývají v závislosti na výrobci či organizaci (například Car to Home je pojem používaný koncernem Volkswagen, zatímco označení Vehicle to Private lze najít ve spojení se společností BMW).

V současnosti byl také zahájen výzkum technologií označovaných jako Rail2X, Ship2X a Airplane2X. Mělo by se jednat o železniční, lodní a letadlovou komunikaci založenou na stejné technologii jako C2X. Jelikož se jedná o kategorie netýkající se silničního provozu, nebudou v této práci dále rozebírány. [3]

2.2 Technické řešení Car-to-X komunikace

Car-to-X samo o sobě nepředstavuje proprietární komunikační technologii, nýbrž se jedná o v některých případech konkrétně specifikovanou a v jiných pouze obecně popsanou výměnu informací, založenou na mnoha různých bezdrátových standardech. Mezi tyto technologie, v závislosti na případu užití, patří rodina standardů pro bezdrátové lokální sítě IEEE 802.11, standard pro celulární sítě LTE či standardy pro nestálou komunikaci na krátké vzdálenosti Bluetooth Low Energy a NFC. Konkrétní technické vlastnosti těchto standardů jsou popsány v následujících příslušných kapitolách. Tato podkapitola slouží pro nastínění principu komunikace vozů se svým okolím v kontextu C2C a C2I (případně C2P).

2.2.1 Obecný princip komunikace

Komunikaci vozů mezi sebou (Car to Car) a komunikaci mezi vozy a infrastrukturou (Car to Infrastructure) lze rozdělit na dva základní a odlišné přístupy. Centrální přístup je založen na směrování veškerých zpráv od vozů a dalších prvků infrastruktury do hlavního komunikačního uzlu (back-end serveru) prostřednictvím již existující mobilní datové sítě. Konkrétně se počítá převážně s využitím technologií 3GPP LTE/LTE-Advanced, v pokrytých lokalitách by se ovšem mohlo jednat například i o WiMAX. Hlavní komunikační uzel v tomto případě může představovat například dopravní řídicí středisko

daného regionu. Tento server přijaté zprávy rozřazuje a zpětně rozesílá těm členům sítě, pro které jsou relevantní. Centralizovaný přístup má svá opodstatněná využití (popsána níže), ale pro plné nasazení na všechny případy užití je technicky příliš složitý a náchylný na poruchy (např. výpadky mobilní datové sítě). Zároveň jsou tímto způsobem Car-to-X komunikace, v místech s vysokou koncentrací provozu, na současné sítě kladeny příliš vysoké nároky na množství přenesených dat. [1], [5]

Mnohem častěji se lze setkat s řešením, které spočívá v lokálním a přímém ad-hoc spojení mezi jednotlivými komunikačními body. Jedná se o decentralizovanou komunikaci, která se obecně (bez ohledu na konkrétní využitou technologii) označuje DSRC[1] (Dedicated Short Range Communications). Fyzickou a linkovou vrstvu pro tuto komunikaci definuje dodatek standardu IEEE 802.11 – 802.11p. V USA se využívá společně s protokolovou sadou IEEE 1609 (která definuje síťovou, transportní a částečně i aplikační vrstvu) pod názvem WAVE (Wireless Access for Vehicular Environments). V Evropě byl adaptován téměř totožný standard Evropským ústavem pro telekomunikační normy (ETSI) pod označením ITS-G5[2]. [6], [7], [11]

Oba standardy operují ve frekvenčním pásmu 5,9 GHz. 75 MHz spektrum v tomto pásmu bylo alokováno americkou Federální komunikační komisí (FCC) výhradně pro DSRC v rámci inteligentních transportních systémů již v roce 1999. WAVE využívá rozpětí 5,85 až 5,925 GHz zatímco ETSI ITS-G5 rozpětí 5,855 až 5,925 GHz. V praxi je frekvenční rozpětí identické, jelikož prvních 5 MHz u WAVE je pouze rezervovaných, bez specifikovaného využití. [6], [7], [8]

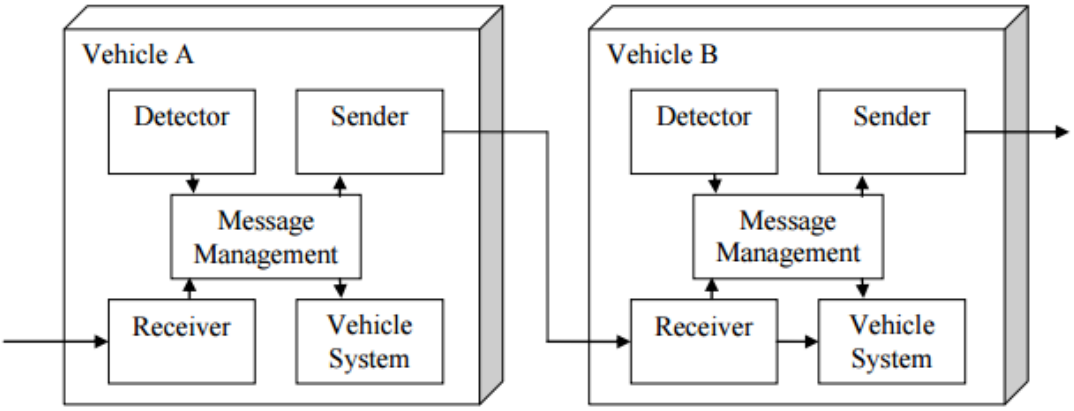
Jednotlivé komunikační uzly v těchto ad-hoc sítích disponují ITS jednotkami, které umožňují příjem, vysílání a dočasné uložení přijatých Car-to-X zpráv. U motorových vozidel se tyto jednotky nazývají On-Board Unit (OBU), jednotky osazené na statických prvcích infrastruktury (např. světelném signalizačním značení, vjezdu do parkovacího domu, čerpací stanice atd.) nesou analogické označení Road-Side Unit (RSU). Ve chvíli,

[1] Zde DSRC představuje obecné označení pro komunikaci daného typu mezi vozy. Evropský výbor pro normalizaci ve standardu EN 300 674 definuje DSRC jako konkrétní technologii operující v pásmu 5,8 GHz pro elektronický výběr mýta – druhá varianta bude v práci pro přehlednost v případě zmínky označována CEN DSRC.

[2] Protokolová sada IEEE 1609, 802.11p a ETSI ITS-G5 jsou podrobněji rozvedeny později v kapitolách 2 a 3.

kdy se dva a více těchto jednotek objeví ve vzájemném dosahu, je mezi nimi automaticky navozeno spojení a začíná konzistentní výměna informací o vzájemné poloze, rychlosti a směru jízdy. Rádiová technologie 802.11p definuje dosah tohoto spojení na teoretických 1000 metrů, po praktických zkouškách však Car 2 Car Communication Consortium stanovilo jako dostatečný přípustný dosah alespoň 300 metrů. Problém krátkého dosahu řeší multi-hop, který umožňuje každé ITS jednotce fungovat jako směrovač a přijatou zprávu o události předat dál. [9], [10]

Šíření zpráv graficky znázorňuje schéma níže (obrázek 1): Přijímač vozidla A přijme zprávu, message manager následně zhodnotí relevanci zprávy a porovná ji s vlastními daty. Vyhodnocuje, že na zprávu vozidlo A samotné nemusí reagovat, nicméně zpráva může být relevantní pro vozidlo B, předává ji tedy vysílači. Přijímač vozidla B zprávu zachytí. Zpráva je vyhodnocena jako bezprostředně relevantní pro vozidlo B, tudíž dochází k předání informací vozu (např. pro možnost akustického varování řidiče) a zároveň dalšímu přeposlání zprávy. [12]



Obrázek 1 - Přenos C2C zpráv mezi více ITS jednotkami pomocí skoků [12]

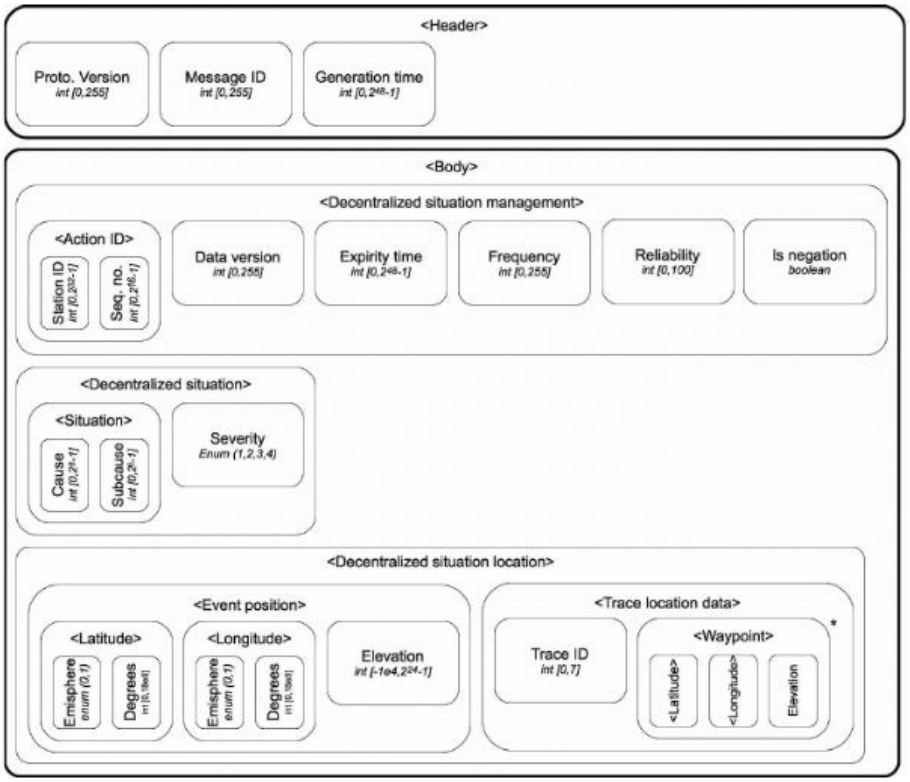
OBU je napojeno na vnitřní síť vozu, kterou v převážné většině případů tvoří CAN bus (Controller Area Network), který umožňuje vzájemnou sériovou komunikaci mezi všemi řídícími jednotkami (ECU) ve voze. Napojení může ovšem být na libovolnou jinou datovou sběrnici vozidla, jakými jsou například FlexRay či Ethernet, případně i více sběrnic zároveň. Ostatní ECU ve voze prostřednictvím této sítě poskytují OBU informace na základě vlastních vstupů (např. navigační data, rychlost jízdy, intenzita brzdění, ztráta

trakce, spuštění výstražných světel atd.). OBU na základě těchto informací vytvoří standardizovanou Car-to-X zprávu a vysílá ji do okolí[3]. Tyto zprávy se dělí na dva základní typy:

- **CAM (Co-operative Awareness Message) –** tuto zprávu každé OBU vysílá s frekvencí 1 až 10 Hz formou single-hop broadcastu. Obsahuje informace o směru jízdy, aktuální pozici a rychlosti daného vozidla. Zpráva dále obsahuje informace o typu a velikosti vozidla a případně další základní informace z jeho senzorů (počet cestujících, akcelerace/brždění/aktivní tempomat, převoz nebezpečného nákladu atd.). Aby nedocházelo k přehlcení komunikačních kanálů, OBU zprávu negeneruje, nedojde-li ke změně úhlu vozu větší než 4º, změně pozice o více než 5 metrů nebo rychlosti o více než 1 m/s. Jelikož aktuálnost zprávy CAM je z její podstaty stěžejní, doba mezi přijetím dat z ostatních jednotek vozu ke zpracování a předáním sestrojené zprávy transportní vrstvě k odeslání nesmí přesáhnout 50 ms. [13], [14], [18]
- **DENM (Decentralized Environment Notification Message)** – Tuto zprávu ITS jednotka vysílá v reakci na konkrétní událost. Mezi tyto události může patřit například prudké brzdění, nehoda či bezprostřední srážka, upozornění na kolonu vozidel, změna viditelnosti. První část zprávy obsahuje řídící informace jako původce zprávy, její verzi (může se jednat o aktualizaci již existující situace), časovou lhůtu její platnosti, jestli zpráva neguje některou z předchozích zpráv a její spolehlivost. Přiřazená spolehlivost v rozsahu 0-100 určuje, jaká je pravděpodobnost, že popisovaná událost v daném místě opravdu nastala a je určena ITS jednotkou původce na základě dat ze senzorů vozidla dostupných v daný moment (message manager příjemce tak může vyhodnotit, zda na zprávu reagovat/přeposlat či zda má čekat na potvrzení v podobě přesnějších údajů). Druhá část obsahuje popis situace (kód události a přiřazený stupeň vážnosti).

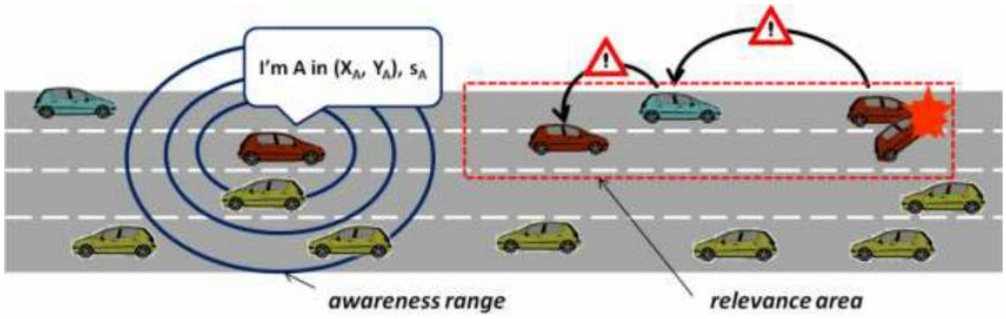
[3] Aplikační sada protokolů pro Car-to-X může být také implementována v separátní řídící jednotce – v tom případě se tato jednotka nazývá Application Unit (AU) a na ní napojené OBU slouží pouze jako jednoduchá komunikační brána. Jelikož se ale toto rozdělení z hlediska architektury vozu jeví jako zbytečné, výraz OBU v kontextu práce vždy představuje plnohodnotné ECU pro C2X komunikaci. [12]

Poslední část obsahuje informace o místu události a přesnosti jeho určení (viz obrázek 3). [13], [16]



Obrázek 2 - Struktura zprávy DENM [17]

Hlavička obou typů zpráv obsahuje jejich rozlišovací znak (0 = CAM, 1 = DENM) a přesný čas vygenerování zprávy. Synchronizace času mezi všemi ITS jednotkami je v síti s neustále se měnící topologií a rychle se pohybujícími uzly stěžejní pro určení validity a místa vzniku zprávy. Maximální celková latence činí u obou typů zpráv 100 ms. Formáty zpráv CAM a DENM jsou relevantní i v kontextu centralizovaného přístupu ke Car-to-X zmíněného na začátku kapitoly, přesun informací se ovšem značně komplikuje, kdy i dvě sousední ITS jednotky komunikují prostřednictvím vzdáleného prostředníka. [13], [15]



Obrázek 3 - Grafické znázornění CAM a DENM [15]

Jak OBU, tak RSU jednotky mohou být kromě 802.11p pro DSRC vybaveny také řadou dalších rádiových technologií, jako například Bluetooth či standardní IEEE 802.11a/b/g/n/ac pro využití pro bezpečnostně nerelevantní komunikaci (např. případy užití týkající se Car to Home). Standardní také bývá možnost připojení k internetu prostřednictvím mobilní sítě, které zejména RSU využívá pro komunikaci s dopravním řídícím střediskem, může však například i poskytovat připojení k internetu všem OBU ve svém okolí. [12]

2.2.2 Zabezpečení a ochrana soukromí

V rámci C2C a C2I komunikace dochází k výměně velmi citlivých dat. Zprávy CAM obsahují data, na základě kterých lze sledovat pohyb specifického vozidla (čas, místo, rychlost, směr). Dopátrání řidiče takového vozu již není složité. Analýza CAM zpráv z vozu tedy umožňuje sledování pohybu konkrétní osoby. Ještě větší problém představuje zneužití zpráv DENM, kde například vysílání falešné zprávy může mít i fatální následky (například přinucení vozidla k nebezpečnému úhybnému manévr). V nejhorším možném případě by mohlo dojít k úplnému převzetí kontroly nad dopravou útočníkem. Bezdrátová forma přenosu informací pak činí Car-to-X komunikaci ještě náchylnější případným útokům. Bezpečnosti C2X komunikace je tedy třeba věnovat obzvlášť vysokou pozornost v rámci všech vrstev, aby byly ošetřeny veškeré rizikové faktory.

V rámci WAVE je zabezpečení řešeno konkrétně standardem IEEE 1609.2. ETSI definuje Security Management, který proniká napříč všemi vrstvami DSRC komunikace, konkrétní implementaci popisovaných metod však nezmiňuje. Bezpečnostní architektura WAVE a ITS-G5 je velmi podobná, stejně jako tomu je u jiných částí standardů. [21], [26]

Public Key Infrastructure pro DSRC

DSRC sítě pro bezpečnost dat nemohou využívat symetrickou kryptografii, jelikož jsou decentralizované a při zveřejnění klíče jedinou ITS stanicí a následné kompromitaci celého systému není způsob, jakým lze klíč všech ITS stanic aktualizovat. V současnosti se tedy plánuje pro DSRC C2X použití Public Key Infrastructure (PKI). Určená certifikační autorita (CA) certifikuje veřejné klíče, které se využívají pro tvorbu digitálních podpisů zpráv. Tyto certifikované klíče tvoří takzvané pseudonymy.

Certifikační autorita, která přidělování pseudonymů zajišťuje, se nazývá Pseudonym certificate authority (PCA). [19], [20]

Pseudonymy slouží kromě zabezpečení a autentizace během komunikace také pro znemožnění identifikace konkrétního vozu v C2X síti. Pseudonym představuje kompromis mezi úplnou anonymitou a zachováním možnosti zpětné rekonstrukce identity vozu v případě nutnosti. Konkrétní vozidlo, které se za ním skrývá, může identifikovat pouze příslušná autorita, která jej vozidlu přidělila, a to pouze ve spolupráci s autoritou, která vozu přidělila dlouhodobý certifikát (viz níže). Úplná anonymita není u komunikujících vozidel přípustná, jelikož musí být zachována možnost odebrání certifikátu (a tím vyjmutí daného vozidla z další komunikace) při zjištění zneužívání systému či kompromitaci certifikátu. Zároveň je vyloučena z principu architektury systému. [19]

Vozům je pseudonymů přidělováno více a každý je časově omezený, důvodem je zamezení možnosti nalezení souvislosti mezi jedním pseudonymem a vozem, který se za ním skrývá. Mezi současné návrhy bezpečnostních architektur patří možnost vozidla udržovat řádově desítky pseudonymů najednou, každý s platností v rozmezí minut až dnů. Problémem této architektury je nutnost datového spojení s backend serverem certifikační autority, které ITS jednotce ve vozidle umožňuje získání nové sady pseudonymů. Čím kratší životností a vyšší frekvencí výměny budou pseudonymy disponovat, tím vyššího stupně anonymizace lze dosáhnout. Vozidlo bude ale muset být častěji připojeno k internetu z důvodu přidělení nové sady. [19]

Kromě pseudonymů (krátkodobých certifikátů) sloužících pro autentizaci ITS jednotky během C2X komunikace, existují také dlouhodobé certifikáty (LTC – Long Term Certificate). Tyto certifikáty vydává Long Term Certification Authority (LTCA) a slouží pro autentizaci ITS jednotky u PCA při žádosti o vydání pseudonymů.[4] O vydání LTC zpravidla žádá výrobce automobilu a jeho platnost trvá po celou životnost vozidla. LTC představuje digitální identifikaci vozu a může obsahovat identifikační parametry jako

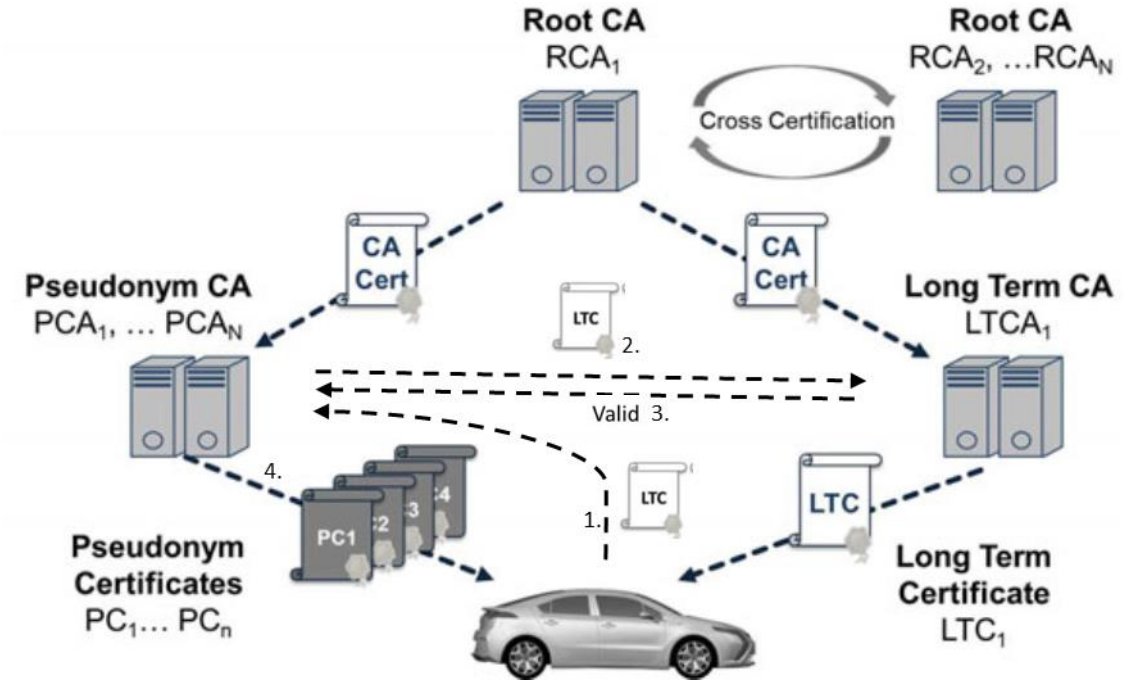
[4] Rozdělení certifikačních autorit znemožňuje jedné z nich sledovat konkrétní vozidlo – PCA nezná vozidlo, kterému pseudonymy vydalo, zatímco LTCA nezná pseudonymy, pod kterými vůz vystupuje.

VIN, z důvodů ochrany soukromí tedy nesmí být použito pro autentizaci C2X zpráv – pro tento účel slouží pseudonymový certifikát. [19], [23]

Nejvyšší entitu v C2X PKI hierarchii tvoří takzvaná Root Certificate Authority (RCA). Role této nejvýše postavené certifikační autority je dohled na dodržování pravidel podřízených certifikačních autorit (LTCA a PCA) a udělování certifikátů umožňujících těmto certifikačním autoritám provoz. Kořenové certifikační autority budou řízeny vládními organizacemi a jejich počet bude limitován na minimum (jedna pro Evropu, jedna v USA atd.). Jednotlivé RCA také mohou vzájemně certifikovat jedna druhou za účelem rozšíření interoperability C2X PKI bezpečnostního řešení ve světě. Celkovou PKI hierarchii znázorňuje obrázek 4. [23]

Obrázek 4 zároveň zjednodušeně popisuje proces žádosti ITS jednotky o pseudonymy:

1. ITS jednotka vozu žádá PCA o přiřazení pseudonymů prostřednictvím svého LTC
2. PCA přeposílá LTC LTCA, které kontroluje platnost LTC a certifikátu PCA
3. LTC je validní a má práva žádat o pseudonymy, LTCA zároveň stanovuje příští interval výměny pseudonymů
4. PCA dle intervalu přiděluje jednotlivým pseudonymům délku platnosti a vydává podepsanou sadu pseudonymů ITS jednotce vozidla



Obrázek 4 - Architektura Public Key Infrastructure pro DSRC [19] s vlastními úpravami

Kontrola plauzibility zpráv

Kryptografické zabezpečení založené na PKI zajišťující důvěryhodnost C2X komunikace při zachování dostatečného stupně soukromí je hlavní, ale nikoliv postačující bezpečnostní opatření DSRC. Další nutnou formou ochrany na aplikační úrovni je kontrola plauzibility zpráv, jelikož zneužití ITS jednotky pro tvorbu falešných zpráv představuje velmi reálnou možnost útoku. K falzifikaci zprávy může dojít například prolomením ochrany vnitřní sítě vozu a posíláním falešných CAN signálů OBU. Data ve zprávě mohou být také poškozena. Kontrola plauzibility spočívá ve vyhodnocení pravděpodobnosti, s jakou je situace, kterou zpráva popisuje, možná. Na základě komplexních algoritmů příjemce vyhodnotí, že zpráva je buďto:

- **Chybná** – data, která zpráva nese, jsou neslučitelná s realitou a ignorována
- **Neutrální** – nelze s přesností určit věrohodnost doručené zprávy
- **Schválena** – Data obsažená ve zprávě prošla všemi kontrolami

Systém může mimo jiné ověřovat následující parametry každé zprávy:

- Udávaná pozice se nachází v dosahu přijímače
- Změna pozice dána dvěma po sobě jdoucími zprávami je z fyzikálního hlediska přijatelná (časově, směrově)
- Udávaná pozice pohybujícího se vozidla se nachází na silnici (kontrola s mapovými podklady)
- Udávaná data neodporují vstupům z ostatních senzorů vozidla (použitelné pouze pro vyhodnocení v bezprostředním a nezakrytém okolí vozidla)

Metody detekce plauzibility zpráv jsou předmětem intenzivního výzkumu, jelikož použití nesprávné implementace může vést k častému vyhodnocení validních zpráv za chybné. Nejvíce náchylná tomuto problému je situace odnikud se objevujícího automobilu, která nastane při nastartování vozu u krajnice či změně pruhu vozu stíněného nákladním automobilem (obr. 5). [19], [25]

Obrázek 5 - Problém náhle se objevujícího vozu při detekci plauzibility zpráv [19]

Zabezpečení v případě centrálního přístupu

V kontextu centrálně řízené C2X komunikace dojde s největší pravděpodobností k využití technologií LTE/LTE-A, které již v základní podobě disponují velmi pokročilými bezpečnostními mechanizmy. Problémem ovšem je, že v současné podobě nevyhovují hlavním požadavkům zabezpečení C2X komunikace. Například předem sdílený symetrický klíč, který LTE pro ochranu mezi koncovým uživatelem a sítí využívá, umožňuje pouze šifrování zprávy, nikoliv kontrolu její integrity (ověření, zda nedošlo k pozměnění dat po odeslání, pro C2X nutné) či věrohodnosti odesílatele. LTE umožňuje i navázání přímého spojení mezi koncovými uživateli, kterým síť poskytne skupinový klíč. V takovém případě nemůže být s jistotou určen konkrétní odesílatel ani zaručena integrita. Zároveň ITS jednotky při komunikaci nemohou čekat na udělení sdílených klíčů. Další problém vzniká v otázce soukromí, jelikož autentizace vůči síti probíhá pomocí unikátního identifikátoru (IMSI – International Mobile Subscriber Identity) přiděleného kartě SIM, kterou musí OBU ve voze obsahovat. Správa této mobilní sítě je v kompetenci operátora, který může z CAM zpráv, které jsou po ní přenášeny, vyčítat velmi přesné informace o lokaci. Data pak lze snadno korelovat s identifikátorem zařízení, které dané zprávy vysílá. Lze tedy očekávat, že na aplikační úrovni centralizované C2X komunikace dojde k adaptaci bezpečnostních opatření již specifikovaných pro DSRC (například v IEEE 1609.2), včetně popisované PKI architektury. [22], [24]

2.3 Standardizace a nasazení Car-to-X

Tato kapitola má za cíl popsat, jaké organizace se podílí na standardizaci Car-to-X a v jaké fázi se standardizace Car-to-X jako celkového systému nachází v globálním měřítku. Zároveň je nutné dodat, že se opět jedná o standardizaci v kontextu inteligentních transportních systémů a bezpečnosti provozu (C2C, C2I, C2P). Komfortní a bezpečnostně nerelevantní případy užití Car-to-X technologie (zpravidla situace při kterých vozidlo není řízeno – odemykání za užití mobilního zařízení, stahování softwarových aktualizací prostřednictvím domácí sítě atd.) si jednotliví výrobci definují sami a nepodléhají speciálním normám.

Hlavním úskalím C2X technologie z hlediska možnosti reálného nasazení je rozpolcenost jejího výzkumu a standardizace, jelikož nutnost použití odlišného hardwarového či softwarového řešení na různých trzích odrazuje výrobce od investování do vývoje a implementace.

V Evropě a Spojených státech amerických, kde by mělo dojít primárně k využití DSRC, je tento problém úspěšně řešen vzájemnou kooperací Evropské komise a Ministerstva dopravy USA (USDOT). V rámci této spolupráce byly založeny specializované pracovní skupiny, které se věnují harmonizaci již existujících DSRC standardů na obou kontinentech a společnému koordinovanému vývoji nových standardů. Touto harmonizací prošly například standardy popisující C2X bezpečnostní zprávy. V USA jsou tyto zprávy popsány ve slovníku základních zpráv SAE J2735 vydávaném standardizační organizací Society of Automotive Engineers. Evropskou sadu zpráv definuje Evropský ústav pro telekomunikační normy (TS 102 637-2 – CAM a TS 102 637-3 – DENM). Přestože tyto sady nejsou identické, jejich podobnost a struktura jednotlivých zpráv umožňuje adaptaci obou variant na jedné ITS jednotce. Stejnému sjednocujícímu procesu podléhají i standardy nižších vrstev, které pro WAVE používaný v USA specifikuje, jak již bylo zmíněno, Institut pro elektrotechnické a elektronické inženýrství (IEEE) a pro CITS v Evropě ETSI. Využívané frekvenční pásmo, bezpečnostní řešení či způsoby směrování jsou tedy podobné, čemuž napomáhá i fakt, že standard ETSI ITS-G5 nevznikl plně nezávisle, ale vychází z IEEE 802.11p. Mezi snahy USA a EU o společný výzkum, vývoj a harmonizaci v oblasti CITS vstoupilo i japonské Ministerstvo pevniny, infrastruktury, dopravy a turistiky, které pro DSRC alokovalo odlišné pásmo 5,8 GHz. [20], [28], [29]

Evropská komise též spolupracuje s organizací CAR 2 CAR Communication Consortium, která mimo jiné reprezentuje privátní sektor. Členy jsou výrobci automobilů, přední vývojové společnosti z oblasti telekomunikací a elektroniky, univerzity a výzkumné instituty. Tato organizace pracuje na otevřeném standardu pro C2X komunikaci založenou na DSRC, propaguje její harmonizaci ve světě a úzce spolupracuje na návrzích řešení a jejich standardizaci s ETSI, kde je zmiňované Consorcium hlavním kontributorem. C2C Communication Consortium zároveň stanovilo milníky plynulého nasazení, které rozdělilo do pěti fází: [20], [27]

1. Systém pro většinový trh podporující základní případy užití a jednoduché CAM/DENM zprávy (prudké brzdění, varování o vozidlu s právem přednosti v jízdě, porouchané vozidlo na cestě, pozice/směr jízdy atd.), pouze formou varování řidiče, žádné automatizované úkony (2020)
2. Nasazení složitějších případů užití jako predikce možné nehody, fúze C2X zpráv a dat ze senzorů vozu, žádná či minimální automatizace (2020 – 2025)
3. Asistenční systémy vozu plně využívají kombinace vstupů ze senzorů vozu a C2X zpráv pro analýzu situace a automatizované zásahy do řízení (2025 – 2030)
4. Kompletní implementace technologie, vzájemná aktivní koordinace provozu na základě dat – technologie připravena pro plně autonomní řízení (>2030)
5. Kompletní převzetí jízdních funkcí, 100% automatizace

Specifikace pro fázi 1 jsou k dnešnímu datu již plně připravené a někteří výrobci již pracují na implementaci, například u koncernu Volkswagen by mělo dojít k nasazení fáze 1 v rozmezí let 2019 – 2020. Specifikace a standardizace dalších fází v současnosti probíhá. [30], [31], [32]

Ke třem hlavním trhům, které se aktivně zabývají C2X komunikací (USA, EU, Japonsko), v poslední době přibyla také Čína. Zde se ovšem vývoj ubírá spíše směrem centralizované C2X komunikace založené na technologii LTE, čemuž napomáhá také fakt, že v Číně zatím neexistuje rezervované frekvenční pásmo pro DSRC. Plány čínské vlády zahrnují kompletní C2X systém umožňující autonomní řízení už v roce 2025. Místní standardizační organizace připravují slovník zpráv vycházející z SAE J2735 a China ITS Industry Alliance (C-ITS) spolupracuje s 3GPP na standardizaci technologie LTE-V umožňující přímou komunikaci mezi vozidly podobající se DSRC. Využití LTE pro C2X je aktivně zkoumáno i v Evropě a Japonsku, zatímco v USA společnost Audi již aplikovala první funkční případ užití C2I založený na LTE[5]. [22], [33], [34]

[5] V určitých městech s centrálním řízením světelných signalizačních zařízení jsou data o intervalech těchto zařízení poskytována společnosti Audi. Vůz se při přiblížení konkrétnímu zařízení (zjištěno prostřednictvím navigačního systému) spojí se servery Audi prostřednictvím LTE a jsou mu poskytnuta data o času do změny signálu na zelenou, což je zobrazeno řidiči. Jedná se o zjednodušenou formu systému GLOSA (Green Light Optimal Speed Advisory), již specifikovanou pro DSRC v Evropě i USA.

3 Technologie využívané pro Car-to-X

Zatímco v předchozí kapitole byla představena technologie Car-to-X jako celek, účelem této kapitoly je blíže seznámit se standardy užívanými pro bezdrátový přenos dat v rámci Car-to-X. Jak již bylo zmíněno, v kontextu DSRC se jedná o technologie založené na rodině standardů bezdrátových lokálních sítí 802.11, zatímco u centrálně řízeného Car-to-X systému především standardy 3GPP třetí a čtvrté generace.

3.1 IEEE 802.11

Jak již bylo zmíněno, technologie normalizovaná standardizačním institutem IEEE, komerčně označována Wi-Fi, je ve své standardní či upravené formě základem pro přenos dat v rámci Car-to-X.

3.1.1 Standardní WLAN

Standard 802.11 byl poprvé publikován v roce 1997, k významnému rozšíření však došlo až o dva roky později, kdy vznikly standardy 802.11b a 802.11a. Standard 802.11b využívá bezlicenčního pásma 2,4 GHz a disponuje maximální přenosovou rychlostí 11 Mb/s. 802.11a operuje v bezlicenčním frekvenčním pásmu 5 GHz a používá OFDM (ortogonální multiplex s frekvenčním dělením). OFDM označuje formu vícenosné modulace, kde je dostupná frekvenční šířka rozdělena na paralelní vzájemně se neovlivňující podkanály, kterými přenášejí jednotlivé bity modulované nosné vlny. Podkanály se vzájemně překrývají, tudíž dochází k maximálnímu využití frekvenční šířky. Přijímač na druhé straně nosné vlny demoduluje a složí dohromady původní informaci. Toto efektivní využití spektra vede ke zvýšení datové propustnosti až na teoretických 54 Mb/s, v závislosti na použité amplitudové či fázové modulaci (BPSK, QPSK nebo 16 a 64-QAM). [36], [38], [40]

Další úprava standardu pro WLAN, 802.11g, přinesla podporu OFDM do pásma 2,4 GHz, čímž došlo ke zvýšení maximální datové propustnosti na 54 Mb/s i v tomto pásmu (v praxi pouze až 24 Mb/s z důvodu zahlcení pásma). Výrazný posun ovšem představuje standard 802.11n, schopný operace v pásmech 2,4 i 5 GHz. Úprava 802.11n umožnila kromě standardních 20 MHz kanálů využití i kanálů o šířce 40 MHz, hlavním přínosem však bylo zavedení metody využívající jevu vícecestného šíření signálu MIMO (Multiple-

input multiple-output). MIMO umožňuje rozdělení dat na více částí a vysílání/příjem každé části více anténami zároveň. Tato metoda umožňuje násobení datové propustnosti v závislosti na počtu antén, v maximální možné konfiguraci čtyř antén na každém komunikujícím zařízení je teoretická propustnost tedy až 600 Mb/s. Nejnovější platný standard je 802.11ac, přinášející podporu 80 a 160 MHz kanálů a až 8x8 MIMO, čistě teoreticky lze dosáhnout rychlostí až 6,93 Gb/s. 802.11ac také umožňuje využití technologie MIMO pro komunikaci s více zařízeními zároveň (MU-MIMO). [35], [37], [39]

Bezdrátové lokální sítě se většinou skládají ze základních útvarů nazývaných Basic Service Set (BSS). Tyto útvary jsou tvořeny přístupovým bodem (AP – access point) a klientskými stanicemi k němu připojenými. Mimo BSS mohou jednotky komunikovat pouze prostřednictvím přístupového bodu. Existují sice BSS i bez AP, stanice v něm obsažené ovšem nemohou komunikovat s nikým mimo daný BSS. To představuje jeden z hlavních důvodů, proč standardní WLAN nemůže být použita pro DSRC komunikaci, kde je potřeba rychlé ad-hoc navození komunikace mezi dvěma stanicemi v dosahu bez zdlouhavé autentizace a asociace s přístupovým bodem. Využitelnost klasických Wi-Fi standardů pro DSRC také mimo jiné limituje operace těchto technologií v bezlicenčních pásmech, ve kterých je velmi vysoké riziko rušení (např. v pásmu 2,4 GHz kromě velkého množství Wi-Fi zařízení operují jiné bezdrátové sítě jako Bluetooth či ZigBee, bezdrátové telefony, imobilizéry, video vysílače a další zařízení.). Wi-Fi je ovšem vhodnou technologií pro přenos dat mezi vozidlem a okolím při statickým situacích, kdy není vyžadováno rychlé spojení a vysoká spolehlivost přenosu (např. Car2Home).

3.1.2 Automotive WLAN 802.11p

Jak již bylo vícekrát zmíněno, standardní WLAN technologie nejsou vhodné pro využití v dynamickém prostředí automobilového provozu, zejména byla nutná možnost komunikace mimo klasický BSS, z tohoto důvodu vzniknul dodatek IEEE 802.11p pro bezdrátovou komunikaci mezi vozy a infrastrukturou. Mezi další změny, které bylo potřeba pro přizpůsobení WLAN pro DSRC implementovat, patří:

- Zvýšení vysílacího dosahu (z přibližných 100 m na až 1000 m)

- Schopnost operace ve vysokých relativních rychlostech (až 500 km/h) a v prostředí s vysokým počtem odrazů signálů
- Schopnost koexistence mnoha překrývajících se ad-hoc sítí

Základ pro 802.11p představuje primárně standard 802.11a, od kterého přebírá většinu fyzické vrstvy, včetně OFDM. Kanály jsou však primárně 10 MHz (oproti 20 MHz u 802.11a)[6], ochranný interval mezi datovými přenosy je naopak dvakrát delší, což pomáhá minimalizovat rušivý efekt opožděných signálů. Tyto změny zvyšují spolehlivost přenosu, což je pro DSRC stěžejní. Související snížení datové propustnosti není pro relativně krátké DSRC zprávy limitující. Dále je také využíváno již zmíněné rezervované pásmo v rozmezí 5,85 až 5,925 GHz namísto velmi zatíženého bezlicenčního pásma 5 GHz, ve kterém operuje 802.11a. Porovnání fyzických vrstev technologií 802.11a a 802.11p je znázorněno v tabulce 1. [41], [42]

	IEEE 802.11a	**IEEE 802.11p**
Rychlost přenosu	6, 9, 12, 18, 24, 36, 48, 54 Mb/s	3, 4,5, 6, 9, 12, 18, 24, 27 Mb/s
Používané modulace	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM
Kódovací poměr	1/2, 2/3, 3/4	1/2, 2/3, 3/4
Počet podkanálů	52 (4 řídící, 48 data)	52 (4 řídící, 48 data)
Doba trvání OFDM symbolu	4.0 µs	8.0 µs
Ochranný interval	0.8 µs	1.6 µs
Šířka kanálu	20 MHz	10 MHz
Frekvenční pásmo	5,170 - 5,825 GHz[7]	5.9 GHz (5.850–5.925 GHz)
Dosah	cca. 120 m	až 1000 m

Tabulka 1 - Srovnání fyzických vrstev standardů 802.11a a 802.11p

[6] V novější revizi standard 802.11p podporuje i 20 MHz kanály pro možnost přenosu větších objemů dat.
[7] Využití konkrétních kanálů v uvedeném frekvenčním rozsahu se v jednotlivých zemích liší v závislosti na regulacích daných telekomunikačních úřadů

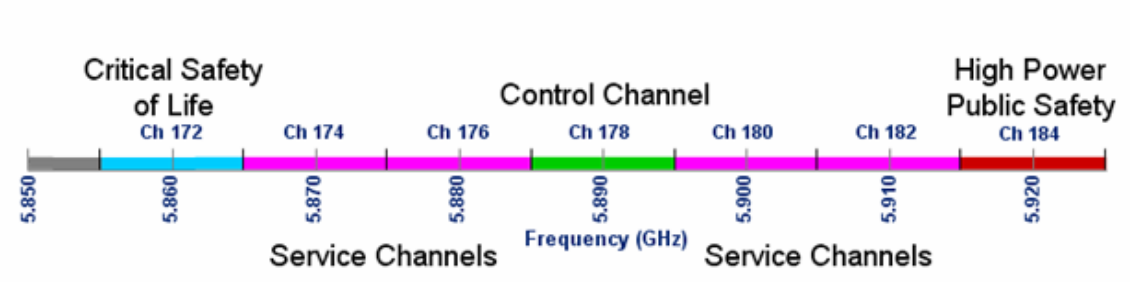
Linkovou vrstvu standard 802.11p též přebírá od 802.11a, společně s vylepšením prioritizace zpráv definovaného v dodatku 802.11e. Základem je metoda EDCA (jedná se o vylepšenou metodu DCF pro sdílení dostupného média založenou na náhodném přístupu ke kanálům), která využívá protokol pro předcházení kolizí CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) založený na naslouchání a soutěžení. Zjednodušeně, uzel, který bude vysílat, naslouchá určitý čas na kanálu. Pokud je kanál po danou dobu volný, vysílá. V opačném případě dochází k náhodnému počtu vyčkání časových úseků (slot time – dvojnásobek času cesty signálu mezi uzly s maximální možnou vzájemnou vzdáleností) v intervalu 0 až CW (soutěžní okno), po jehož vypršení se uzel může pokusit o další přenos. Je-li kanál opět obsazený, soutěžní okno je postupně exponenciálně zvětšováno od CW_{min} až po CW_{max}, přičemž při úspěšném odeslání dochází k resetování soutěžního okna na hodnotu $CW_{min.}$ [41], [43]

Zatímco standard 802.11a definoval hodnoty CW_{min} a CW_{max} pevně na 15, respektive 1023, 802.11p z důvodu přísných požadavků na nízkou odezvu využívá rozdělení hodnot dle priority od nejvyšší po nejnižší na CW_{min} = 3, 7, 15, 15 a CW_{max} = 7, 15, 1023, 1023, definované v 802.11e. Čas, po který uzel naslouchá, zdali je médium volné, je též variabilní v závislosti na prioritě. Zároveň, 802.11p rámce vysílané formou broadcastu (používaného pro bezpečnostně relevantní zprávy) nevyužívají exponenciálního zvětšování soutěžního okna, v tomto případě má CW vždy hodnotu CW_{min}, kritické zprávy tedy mají vždy výhodu minimálního možného čekání. Slot time je u automotive WLAN naopak z důvodu zvýšeného dosahu delší (13 µs oproti 9 µs u výchozího 802.11a). [41], [44]

Automotive WLAN se od klasického také značně liší v adresaci. Mezi stanicemi (RSU nebo OBU) neexistuje žádná hierarchie (přístupový bod – klient) a připojují se mezi sebou napřímo. RSU jednotky disponují klasickou pevně danou 48 bitovou MAC adresou, MAC adresa OBU se ovšem generuje náhodně při probuzení dané jednotky, v případě kolize MAC adres dochází ke generaci nové. [41], [42]

75 MHz pásmo, které WAVE využívá, je rozděleno na rezervované, 5 MHz ochranné pásmo a sedm nepřekrývajících se 10 MHz kanálů. Kanály se dělí na dva základní druhy – servisní kanály (SCH) a kontrolní kanál (CCH). Servisních kanálů je celkem šest a

slouží pro bezpečnostní i bezpečnostně nerelevantní užití (v závislosti na konkrétním kanálů). Kanál 172 je určen výhradně pro bezpečnostně relevantní C2C komunikaci a lze v něm vysílat výkonem až 33 dBm. Stejnou hodnotou maximálního vysílacího výkonu disponují kanály 174 a 176 pro poskytování služeb na střední vzdálenost, u kterých existuje možnost spojení do jednoho 20 MHz kanálu pro zvýšení datové propustnosti. Možnost spojení nabízí i kanály 180 a 182 pro komunikaci na krátké vzdálenosti s maximálním vysílacím výkonem 23 dBm. Poslední servisní kanál, č. 184, slouží pro bezpečnostně relevantní komunikaci na větší vzdálenosti a lze v něm vysílat s výkonem až 40dBm. Kontrolní kanál 178, s maximálním vysílacím výkonem 44,8 dBm, je umístěn ve středu DSRC spektra a rezervován pouze pro krátké broadcast zprávy s vysokou prioritou týkající se bezpečnostně kritických situací vyžadujících minimální latenci či inicializace komunikace po SCH. SCH kanály umožňují komunikaci založenou na IPv6 protokolu a UDP/TCP, primárně však probíhá komunikace mimo IP, využívající WAVE Short Message Protocol (WSMP) standardizovaný normou IEEE 1609.3. Komunikace po CCH probíhá pouze prostřednictvím WSMP. [41], [45]



Obrázek 6 - Rozložení kanálů ve vyhrazeném DSRC spektru [45]

ETSI ITS-G5 využívá stejných sedmi kanálů v DSRC pásmu, pouze s odlišným uspořádáním (např. CCH na kanálu 180) a výkonovými limity. ITS-G5, oproti WAVE, dále definuje variabilní sedmý SCH v bezlicenčním 5GHz pásmu. ITS-G5 je technologii WAVE obzvláštně na PHY a MAC vrstvě natolik podobné, že nemá smysl v kontextu této práce daný standard více rozebírat. [6]

3.2 3GPP LTE a LTE-A

Technologie LTE se v kontextu Car-to-X považuje za hlavní alternativu pro 802.11p. Je tomu tak především z důvodu, že tato technologie eliminuje řadu nevýhod, které se týkají DSRC komunikace – nízký dosah omezující případy užití, hrozba kolizí v prostředí s vysokým počtem uzlů či nemožnost přenášet větší objemy dat.

LTE, celým názvem Long Term Evolution, je standard specifikovaný a vydaný spolupracující skupinou telekomunikačních asociací 3rd Generation Partnership Project. Představuje postupný přechod z 3G sítí na plnohodnotné 4G sítě, jejichž parametry bude splňovat standard LTE Advanced, který se po té s přídavkem Pro též stane překlenovacím směrem k 5G sítím. Jedná se o specifikace standardních celulárních sítí založených na technologiích GSM a UMTS a využívajících pro komunikaci protokol IP. Koncová zařízení se tedy v síti identifikují a autentizují pomocí unikátního identifikátoru IMSI uloženého na kartě SIM a komunikují se základnovou stanicí buňky, ve které se v daný moment nachází. Základnové stanice tvořící jednotlivé buňky sítě jsou zároveň napojeny na ústředny provozovatele dané sítě, které je propojují navzájem a s jinými sítěmi. [46]

LTE operuje v závislosti na regionu a dostupnosti v pásmech mezi 700 MHz a přibližně 3 GHz, přičemž využívá kanály různých šířek od 1,4 po 20 MHz a pro přenos může využívat duplexní spojení s časovým i frekvenčním dělením. Pro vysílání směrem od základnové stanice ke koncovým zařízením je využívána metoda OFDMA, která umožňuje aplikovat rozdělení frekvenční šířky do nezávislých modulovaných nosných vln, OFDM, na přenos směrem k více uživatelům. Přenos opačným směrem (uplink koncových zařízení) je realizován mírně se lišící metodou SC-FDMA, která disponuje nižším poměrem špičkového a průměrného vysílacího výkonu a tudíž šetří akumulátory zařízení. LTE též implementuje MIMO, což zvyšuje efektivitu využití spektra oproti předchozím technologiím až čtyřnásobně. V důsledku, LTE může dosahovat teoretických rychlostí přenosu až 300 Mb/s (downlink) při využití 20 MHz kanálu a MIMO. Nadcházející technologie LTE Advanced rozšiřuje oblast použitelných pásem na 450 MHz až téměř 5 GHz, využívá až 100 MHz kanálů a mělo by nabízet ještě vyšší efektivitu využití spektra, docílenou například dalšími vylepšeními metody MIMO. Teoretická přenosová rychlost LTE-A činí 1 Gb/s. [15], [47]

Problém s nasazením LTE řešení pro Car-to-X je zejména nepřipravenost celulárních technologií pro takové využití (standardy pro DSRC jsou připravovány mnoho let a již technicky realizovatelné). LTE v současnosti nesplňuje nároky na zabezpečení, anonymitu či přísné požadavky na nízkou latenci (zpráva musí projít základnovou stanicí, než může být redistribuována adresovaným ITS jednotkám). Problém představuje i pokrytí a spolehlivost přenosu na delší vzdálenosti, popřípadě přetížení sítě. Lze však očekávat, že problémy s latencí budou s příchodem 4G LTE-A standardu, případně jeho nástupce směrem k plnohodnotným 5G sítím, eliminovány. Potíže s pokrytím a kapacitou sítě by též měly být v blízké budoucnosti přirozeně vyřešeny rychlým rozvojem a výstavbou infrastruktury mobilních sítí. V neposlední řadě, standardy aplikační vrstvy Car-to-X komunikace vyvinuté pro DSRC, jakými jsou například slovník zpráv či PKI zabezpečení, lze mírnými modifikacemi přenést na celulární technologie.

Je také nutné zmínit existenci LTE-V určeného pro lokální komunikaci mezi vozidly odpovídající DSRC. V době vzniku této práce probíhá raná fáze specifikace tohoto standardu, který by měl být založen na LTE-D2D, které umožňuje přímé spojení mezi dvěma a více zařízeními v rámci LTE sítě, LTE síť však těmto zařízením musí nejdříve alokovat zdroje, což zvyšuje latenci. Existuje i autonomní režim umožňující zařízením alokovat si zdroje samostatně, tento režim ovšem vede ke kolizím a rušení. Bezpečnostní nedostatky současného D2D řešení v rámci LTE již byly zmíněny v kapitole 2.2.2. [22]

4 Analýza rizik

V této kapitole je řešena spolehlivostní analýza zjištěných rizik týkajících se Car-to-X technologií a její vyhodnocení. Obsahem je představení metody zvolené k analýze, stanovení parametrů kritičnosti a diskuze nad body vyplývajícími ze samotné analýzy.

4.1 Zvolená metoda analýzy – FMECA

Pro analýzu problémů a rizik spjatých s Car-to-X komunikací byla v této práci zvolena metoda FMECA – analýza způsobů, důsledků a kritičnosti poruch (v originálním znění, z kterého zkratka vychází, Failure Mode, Effects and Criticality Analysis). Jedná se o metodu rozšiřující analýzu FMEA o semikvantitativní[8] složku hodnocení pravděpodobnosti, následků a případně odhalitelnosti jednotlivých poruch. FMEA byla zprvu vyvinuta v armádě Spojených států amerických pro možnost zkoumání důsledků selhání vojenských systémů. Později byla využívána například při přípravě letů na Měsíc, načež došlo k rozšíření jejího užití do dalších průmyslových odvětví, včetně automobilového, kde má široké využití pro analýzu jednotlivých výrobků i procesů. Dnes existuje mnoho norem, které předepisují rozsah a obecný postup analýzy, mezi známějšími například IEC 60812 či SAE J1739. FMEA/FMECA se často využívá v rané fázi vývoje a návrhu komponenty či systému, tvoří tedy ideální metodu pro zjištění způsobů problémů a jejich důsledků v kontextu technologie Car-to-X, která se v současnosti nachází právě v předvývojové fázi. [49]

FMECA je induktivní semikvantitativní analýzou, kde je rozbor prováděn od nižší úrovně k vyšším. Zkoumány jsou tedy jednotlivé komponenty či funkce a jaký vliv má jejich selhání na provoz celkového systému. Definovány jsou tři základní druhy – konstrukční, procesní a systémová FMEA/FMECA. Pro rozbor Car-to-X komunikace bude použita FMECA systémová, jelikož bude analyzována technologie Car-to-X jako celek, skládající se z různých subsystémů a komponent, jejichž individuální selhání či nesprávné chování při jejich vzájemné interakci může ohrozit funkci celého systému. Postup pro metodu FMECA se standardně rozděluje na tři části – přípravnou, samotnou FMECA analýzu prvků systému a závěrečné vyhodnocení výsledků. [48]

[8] Jedná se o hodnocení za užití semikvantitativních hodnot vyjádřených kvantitativně.

Formální zápis analýzy FMECA je proveden pomocí tabulky – každý řádek obsahuje minimálně komponentu systému a její funkci, příčinu její poruchy a následek pro systém. Cílem analýzy je zhodnotit důsledky zjištěných poruch jednotlivých součástí systému, určit jejich kritičnost vzhledem k efektu na požadovanou funkci či bezpečnost celku a následně navrhnout možnosti zamezení či minimalizace těchto negativních důsledků. Výstupem jsou například návrhy konstrukčních změn systému či identifikace nebezpečných situací.

4.2 Přípravná fáze analýzy

V přípravné části je potřeba především stanovit cíle, ke kterým má analýza směřovat a stanovit spolehlivostní požadavky na zkoumaný systém. Součástí je také popis technických parametrů systémů a definice funkcí jeho dílčích součástí. Dále je třeba zvolit úroveň, na které bude systém analyzován v závislosti na jeho komplexitě a znalosti způsobu poruch na jednotlivých úrovních systému.

Cíle analýzy

Hlavním cílem analýzy Car-to-X komunikace v této práci je identifikovat rizika, která mohou vést k technickému selhání systému, jeho zneužití či například kompromitaci soukromí jeho uživatelů. Analýza by měla odhalit zásadní nedostatky ohrožující bezpečnost či spolehlivost systému a navrhnout opatření pro jejich odstranění či minimalizaci. Jelikož analyzovaná technologie se týká bezpečnosti provozu motorových vozidel a je zamýšleno její využití pro aktivní zásahy asistenčních systémů do řízení vozidel či plně autonomní řízení na základě vstupů, které poskytuje, je obzvláště důležitá eliminace rizik před širším nasazením technologie do provozu.

Popis analyzovaného systému a definice funkcí

Technické principy a funkce technologie Car-to-X jsou rozebrány v kapitole 2, ve které se zároveň nachází odkazy na specifikace. Kapitola 3 obsahuje podrobnější popis bezdrátových technologií, které jsou technologií Car-to-X využívány. Podrobný výčet funkcí a prvků systému, včetně poruch, kterým mohou podléhat, je obsažen v samotné FMECA analýze, přičemž podstatnější z nich budou blíže představeny ve vyhodnocující diskuzi.

Volba struktury a úrovně analýzy

Vzhledem k možnosti využití více přístupů pro realizaci Car-to-X bude analýza rozdělena do tří základních kategorií – rizika spjatá s DSRC komunikací založenou na 802.11p, rizika související s řešením založeném na centrální infrastruktuře a rizika týkající se Car-to-X komunikace obecně, nehledě na zvolenou metodu přenosu informací. Co se týče samotné hloubky analýzy systému, vzhledem k jeho celkovému rozsahu budou základní jednotky analýzy tvořit jednotlivé funkce, úkony a komponenty přispívající k jeho celkové funkčnosti. Hlubší analýza by již vedla k dekompozici jednotlivých komponent tvořících Car-to-X infrastrukturu (např. na jednotlivé díly, ze kterých se skládá jednotka OBU), což by vedlo k přílišné komplexitě analýzy a způsobilo výrazný odklon od cílů zhodnotit koncept realizovatelnosti celkového systému. Zároveň by se již jednalo o doménu konstrukční FMECA analýzy konkrétních komponent na základě jejich dokumentace.

4.3 Návrh tabulek kritičnosti

Základním požadavkem pro správné provedení analýzy FMECA je stanovení kvantifikovatelného hodnocení rizika jednotlivých způsobů poruch. K tomu se využívají číselné ukazatele pravděpodobnosti, následků a případně odhalitelnosti. Existují dvě základní metody vyhodnocení rizika. Jednou z nich je riziková matice, u které řádky vyznačují jednotlivé úrovně pravděpodobnosti výskytu problému, zatímco sloupce úrovně závažnosti následků způsobených daným problémem. Jednotlivé souřadnice matice pak nabývají různých hodnot přípustnosti rizika. Druhá metoda spočívá ve vyhodnocení rizikového čísla RPN, které představuje součin ukazatelů pravděpodobnosti, následků a odhalitelnosti.

Pro analýzu Car-to-X komunikace bude aplikována metoda výpočtu rizikového čísla. Standardně se pro každý ukazatel používá desetistupňové ohodnocení, v tomto konkrétním případě však nelze s přesností ukazatele rozdělit na takový počet hodnot, aniž by byla do analýzy při snaze určit hodnoty zavedena chyba. Pro tak přesné určení jednotlivých hodnot neexistuje dostatek dat ze zkoušek či provozu Car-to-X technologií, analýza je primárně založena na teoretických předpokladech a empirických poznatcích

z funkce bezdrátových technologií, na kterých je Car-to-X založeno. V tomto případě tedy bude použita stupnice pětistupňová.

Tabulka závažnosti následků

Pro možnost kvantifikace následků jsou pro každý stupeň závažnosti stanoveny také zástupné číselné hodnoty. Tyto hodnoty reprezentují finanční náklady, které by mohly vzniknout například výrobci automobilů či jinému dodavateli Car-to-X systému a jeho komponent, pokud by došlo k poruchám o různých stupních závažnosti. Zástupné hodnoty byly určeny na základě finanční zátěže, kterou lze pro nápravu či omezení škod obecně očekávat vzhledem k podobným historickým případům různých rozměrů.

Zástupná hodnota nízkého stupně následků například představuje přibližné náklady spojené se vznikem drobné dodatečné softwarové aktualizace řídící jednotky o velikosti jednoho megabytu a její distribuci milionu vozidel při průměrné ceně dat, zatímco u středně závažných následků lze počítat s nutností rozsáhlejších softwarových či hardwarových úprav. U vysokého stupně následků lze předpokládat nutnost okamžité nápravy problému, spojené s hromadným svoláním vozidel do servisů, přibližná hodnota je zde opět vztažena k milionu vozidel. V nejhorším případě má výpadek či zneužití systému vliv na bezpečnostní technologie ve voze – v případě nalezení souvislosti mezi těžkým zraněním či smrtí způsobenými absencí kritických Car-to-X dat (či jejich manipulací třetí stranou) u daného bezpečnostního prvku lze tedy očekávat i hromadnou žalobu podobající se například té, která postihla firmu Takata, jejichž vzdušné bezpečnostní vaky způsobily 17 smrtí. Výše vyrovnání v tomto případě činila přibližně 25 miliard Kč [50] a je použita jako referenční hodnota pro nejvyšší stupeň následků (pro srovnání, vyrovnání ve věci Dieselgate činilo pro společnost Volkswagen v USA 362 miliard Kč, velmi nákladný výkup vozidel je však ve věci Car-to-X krajně nepravděpodobný). [51]

Následky	Popis	Zástupná hodnota [Kč]	Klasifikace
Žádné	Žádné pozorovatelné důsledky.	0	1
Nízké	Dochází ke sporadickým výpadkům komunikace, některá komfortní využití technologie nejsou k dispozici. Omezení se netýkají bezpečnostně relevantní komunikace. Vliv na uživatele vozidla je minimální – může být mírně nespokojen. Možnost potřeby vydat nápravnou SW aktualizaci.	20 000 000	2
Střední	Komfortní komunikace je značně omezená či nefunkční, případně dochází k nedoručení některých bezpečnostně relevantních zpráv (např. nedochází k vysílání či příjmu CAM) – omezení plynulé funkce některých asistenčních systémů (autonomní řízení by nebylo možné). Nutnost vydání softwarové záplaty či úpravy během pravidelné servisní prohlídky.	1 000 000 000	3
Vysoké	Systém je nefunkční od zahájení jízdy (uživatel je s faktem seznámen) nebo značně omezená možnost komunikace během jízdy, asistenční systémy nemají k dispozici spolehlivá C2C a C2I data - snížení bezpečnosti provozu. Případná kompromitace anonymity uživatele. Pro nápravu nutné uspořádání svolávací akce.	10 000 000 000	4
Nebezpečné	Kompletní výpadek funkčnosti systému během probíhající jízdy či prolomení jeho zabezpečení a zneužití systému třetí stranou (převzetí kontroly nad řízením infrastruktury, vysílání falešných zpráv napadenému vozidlu, atd.). Ohrožuje posádku vozidla či více vozidel na zdraví a životě. Riziko hromadné žaloby vůči dodavateli systému.	25 000 000 000	5

Tabulka 2 - Závažnost následků

Tabulka pravděpodobnosti výskytu

Jelikož některé jevy mohou nastávat téměř neustále (kolize při komunikaci více zařízení po stejném médiu) a některé lze očekávat maximálně jednou za životnost vozidla (selhání jednotky OBU), bude pro stanovení hodnot jednotlivých stupňů pravděpodobnosti výskytu použita geometrická stupnice.

Kvalitativní popis	Pravděpodobnost výskytu 1/h	Četnost výskytu	Klasifikace
Nepravděpodobný výskyt poruchy za životnost vozu[9]	$(0;1 \times 10^{-4}]$	≤ 0,1 na tisíc hodin provozu	1
Nízká: Ojedinělá porucha	$(1 \times 10^{-4};1 \times 10^{-3}]$	> 0,1 až 1 na tisíc hodin provozu	2
Střední: Občasné poruchy	$(1 \times 10^{-3};1 \times 10^{-2}]$	> 1 až 10 na tisíc hodin provozu	3
Vysoká: Dochází k opakování dané poruchy	$(1 \times 10^{-2};1 \times 10^{-1}]$	> 10 až 100 na tisíc hodin provozu	4
Velmi vysoká: porucha se opakuje během každé jízdy	(0,1;1]	> 100 na tisíc hodin provozu	5

Tabulka 3 - Pravděpodobnost výskytů

Tabulka odhalitelnosti události

Určit s přesností faktor odhalitelnosti je v tomto případě složité i na pětistupňové škále, jelikož úplný výpadek komunikace je snadno odhalitelný (nejsou k dispozici žádné související služby, hardwarová porucha s diagnostickou chybou atd.), zatímco například sporadické ztráty CAM a DENM rámců jsou pro uživatele nepostřehnutelné, přičemž je v daný moment snížena účinnost bezpečnostních systému ve voze (daná data nejsou k dispozici). Z toho důvodu bude pro odhalitelnost postačovat pouze třístupňová škála.

[9] Doba provozu vozidla byla odhadnuta na 4380 hodin (5% z celkové doby životnosti, která byla uvažována deset let)

Nicméně, aby nedošlo ke snížení váhy faktoru odhalitelnosti nežádoucího jevu oproti následkům a pravděpodobnosti, použitá stupnice nabývá hodnot 1, 3 a 5 (namísto 1 až 3).

Pravděpodobnost odhalení	Popis	Klasifikace
Vysoká	Vysoká pravděpodobnost, že nežádoucí jev bude v provozu odhalen.	1
Střední	Středně velká pravděpodobnost, že nežádoucí jev bude v provozu odhalen.	3
Nízká	Pravděpodobnost odhalení nežádoucího jevu během provozu je velmi nízká či není možnost detekce.	5

Tabulka 4 - Odhalitelnost události

Tabulka celkového rizika

Součinem hodnot z výše zmíněných škál vznikne celková hodnota rizikového čísla RPN. Při zvolených stupnicích může RPN nabývat 75 hodnot v intervalu [1;125], z toho 28 unikátních.

Jelikož většina možných součinů se pohybuje v první třetině celkového rozsahu, intervaly míry rizika jsou zvoleny nerovnoměrně, přičemž je roztřídění upraveno tak, aby nebylo možné klasifikovat poruchy s hodnotou RPN, které mohou vzniknout součinem maximálních hodnot dvou faktorů, jako méně než vysoce rizikové.

Riziko	Hodnota RPN
Zanedbatelné	1 až 4
Nízké	5 až 10
Střední	11 až 24
Vysoké	25 až 60
Neakceptovatelné	61 až 125

Tabulka 5 - Intervaly celkového rizika

4.4 FMECA rizikových prvků sytému

V rámci přípravné fáze bylo identifikováno celkem dvacet rizikových stavů, které vstoupily do analýzy, přičemž jsou rozebírány rizika aktuální, nikoliv rizika již současnými standardy vyřešena. Samotná analýza se skládá ze standardních položek – mód poruchy, příčina poruchy, následek na systém, opatření a číselné faktory RPN. Vzhledem ke svému rozsahu a formátu je analýza umístěna v příloze této práce, zde je pro orientaci uvedena ve zkrácené podobě, jež neobsahuje příčiny, následky a navrhovaná opatření daných poruch.

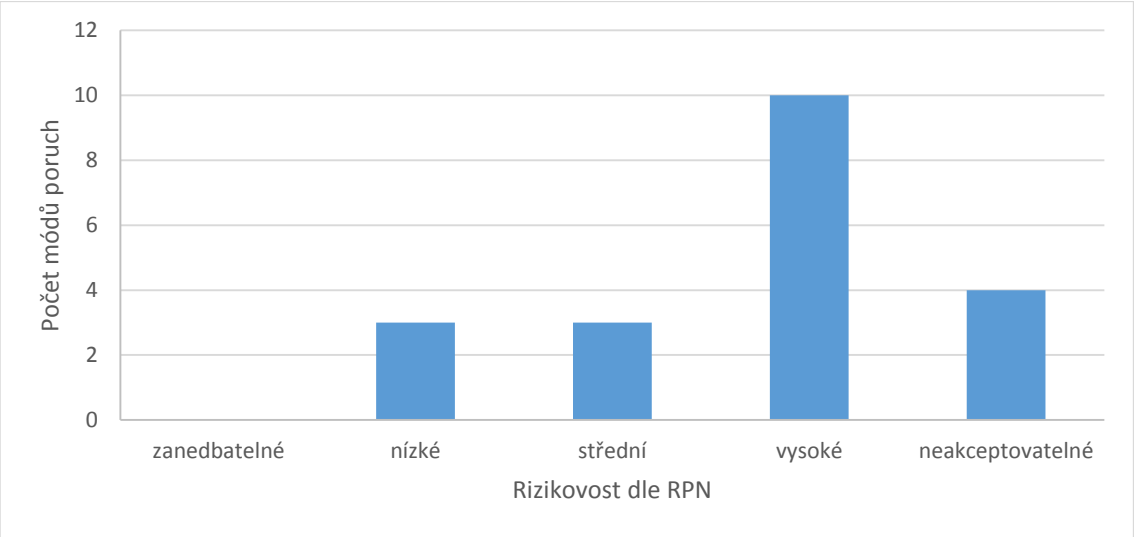
Skupina	Funkce/ prvek	Pol.	Mód poruchy	N	P	O	RPN
Obecné	ITS jednotka	1.1.1	Selhání elektroniky jednotky	5	1	1	**5**
		1.1.2	Používání certifikované jednotky mimo vozidlo či stanici, pro kterou je určena.	5	2	5	**50**
		1.1.3	Překročení výpočetní kapacity	5	3	5	**75**
	GNSS jednotka	1.2.1	Odesílání falešných pozičních dat OBU ke zpracování	5	2	5	**50**
	Vnitřní síť vozu	1.3.1	Překročení maximálního času pro konstrukci zprávy	2	2	3	**12**
		1.3.2	Poskytování falešných signálů OBU pro tvorbu C2X rámců	5	2	3	**30**
	Interoperabilita	1.4.1	Vzájemná nekompatibilita C2X technologií	3	2	1	**6**
DSRC C2X	PKI zabezpečení	2.1.1	Nedojde k obnovení propadlých krátkodobých pseudonymových certifikátů	4	4	1	**16**
		2.1.2	Kompromitace identity žadatele o certifikáty	4	2	5	**40**
	Plné pokrytí okolí vozu signálem	2.2.1	Nepokrytí prostoru před vozem signálem	4	2	3	**24**

	Vysílání v rezervovaném pásmu 5,9 GHz	2.3.1	Zahlcení média	4	5	5	**100**
		2.3.2	Odeslaný rámec nedoručen vzdáleným příjemcům	3	4	5	**60**
		2.3.3	Frekvenční rušení	2	1	5	**10**
		2.3.4	Cílené frekvenční rušení	5	2	5	**50**
LTE C2X	Zabezpečení a ochrana soukromí	3.1.1	Není zajištěna důvěrnost vůči provozovateli sítě	4	3	3	**36**
		3.1.2	Není zajištěna integrita při komunikaci v síti	5	3	5	**75**
	Vysílání v celulární síti	3.2.1	Přetížení síťové infrastruktury	3	3	5	**45**
		3.2.2	Zahlcení média	4	2	5	**40**
		3.2.3	Ztráta spojení	5	5	3	**75**
		3.2.4	Překročení maximální latence	3	2	5	**30**

Tabulka 6 - Zkrácená podoba analýzy FMECA

4.5 Vyhodnocení analýzy a diskuze opatření

Jak již bylo zmíněno, bylo identifikováno celkem dvacet módů poruch, které v současnosti ohrožují nasazení Car-to-X technologií. Jak ukazuje graf, většina identifikovaných rizik byla klasifikována jako vysoká, přičemž čtyři problémy dokonce vedou k rizikům neakceptovatelným. Celkem osm problematických stavů bylo hodnoceno faktorem následků pět – tudíž rizikem velmi závažných důsledků (úplný výpadek komunikace, zlomyslný útok na účastníky provozu atd.), které mohou znamenat pro výrobce C2X komponentů, provozovatele C2X služeb a především výrobce automobilů velmi nákladnou minimalizaci škod a nápravu.



Obrázek 7 - Rizikovost zjištěných módů poruch

Skutečnost, proč byla většina problémů klasifikována jako vysoce či neakceptovatelně riziková a zároveň nebyla objevena zanedbatelná rizika, lze částečně vysvětlit faktem, že většina méně rizikových problémů byla za posledních deset let probíhající standardizace již normami ošetřena. Určitý faktor lze ovšem přisoudit prostředí automobilového průmyslu s vysokými nároky na bezpečnost, z čehož vyplývá nutnost přísného hodnocení módů poruch.

Pro každý poruchový stav bylo v analýze navrhnuto jedno či více opatření, která by mohla vést ke značné minimalizaci daného rizika. V následujícím textu jsou u vysokých a nebezpečných rizik poruchy a navržená opatření diskutována, včetně jejich realizovatelnosti z technického či finančního hlediska. Poruchy v diskuzi jsou řazeny do logických celků na základě vzájemných souvislostí, ne striktně dle nabytého RPN.

4.5.1 Zahlcení média

Zahlcení pásma DSRC 5,9 GHz

2.3.1	Zahlcení média	4	5	5	**100**

Z provedené analýzy vyplývá, že největší problém bránící technologiím založeným na lokální decentralizované komunikaci představuje zahlcení média. Tento problém získal hodnotu RPN = 100 především z důvodu, že při vyšším počtu uzlů, které sdílí médium

v jedné lokalitě, lze očekávat téměř neustálé obsazení kanálů pásma 5,9 GHz s velmi vysokou pravděpodobností. Například z měření [44] vyplývá, že při nominální přenosové rychlosti 6 Mb/s, intervalu vysílání CAM 100 ms a velikosti paketů 200 bajtů dochází k zahození a nedoručení paketů již při počtu sedmi uzlů ve vzájemném dosahu. Citovaný experiment byl proveden ve statickém a uzavřeném laboratorním prostředí a nebyly simulovány žádné náhlé situace (nedošlo k vysílání DENM), lze tedy předpokládat, že v reálných podmínkách bude výsledek horšího charakteru. Zároveň mají bezpečnostně relevantní zprávy při pokusu o odeslání výhodu minimálního CW, CAM a většina v současnosti definovaných DENM je ovšem bezpečnostního charakteru a tyto zprávy tvoří většinu C2X komunikace. Reálná výhoda těchto paketů při pokusu o odeslání je tedy zanedbatelná, přičemž globálně nízké CW způsobuje zvýšení kolizí a další zahlcení sítě.

V rámci analýzy byla navržena řada opatření, která by měla vést k uvolnění sdíleného média, tato řešení ovšem způsobují jiné problémy:

- **Použití vyšší přenosové rychlosti** – Standardní zvolená rychlost pro C2X komunikaci je v současnosti 6 Mb/s, standard přitom umožňuje rychlost přenosu až 27 Mb/s. Nabízí se tedy zvýšení této rychlosti, jelikož čím méně času přenos rámce trvá, tím méně času je médium vysílačem obsazeno. Nevýhodou ovšem je, že vyšší přenosové rychlosti vynucují použití složitějších modulačních schémat (viz tabulka 1), která jsou více náchylná na rušení, čímž se zvyšuje bitová chybovost, je ztížena demodulace na straně příjemce a snížen dosah, jak uvádí i [44]. Řešením může být kompromis – zvýšení přenosové rychlosti na 9 Mb/s. Pro tuto rychlost se používá fázová modulace QPSK stejně jako u 6 Mb/s. QPSK nemá takový sklon k rušení, jako u vyšších rychlostí používaná kvadraturní amplitudová modulace QAM, kde je malá separace mezi stavy.
- **Snížení velikost CAM paketů** – Rámec CAM může obsahovat mnoho informací včetně například úhlu zatočení volantu, stavu světel, šířky vozidla či informaci o nebezpečném nákladu. Omezením parametrů vysílaných v CAM rámci lze docílit výrazného snížení jeho datové velikosti a tím urychlit dobu jeho přenosu. Z teoretického hlediska lze CAM zredukovat pouze na základní informace o

poloze, rychlosti, směru jízdy a prioritě vozidla. S každým vyjmutým parametrem se ovšem snižuje vzájemný kontextuální přehled vozidel a schopnost vozidel předvídat situaci na vozovce, což vede ke snížení celkové bezpečnosti dopravy. S odebíráním parametrů je tedy třeba nakládat velmi opatrně, jelikož čím více detailů o sobě vozy mají, tím lépe mohou automatické systémy na vzniklé situace reagovat.

- **Snížení frekvence odesílání CAM paketů** – počítá-li se s dosahem 300 metrů, může médiem v bodě na plně zaplněné dálnici procházet až 2400 CAM zpráv za sekundu (240 vozů kolem zvoleného bodu, frekvence 10Hz). V takovém prostředí lze očekávat mnoho kolizí. Jednoduchým snížením této vysílací frekvence například na polovinu lze docílit výrazného uvolnění pásma. Při snížení této frekvence lze ovšem opět očekávat snížení bezpečnosti provozu – při zvolení minimální frekvence 1Hz se vozidlo jedoucí rychlostí 130 km/h mezi každou odeslanou zprávou přemístí o více než 36 metrů, čímž se stávají přenášené údaje téměř nepoužitelné. Nelze tedy doporučit snížení frekvence o více než polovinu, přičemž je nutností implementace algoritmu pro předpověď reálné pozice vozidla na základě rychlosti, směru jízdy a intervalu mezi zprávami.
- **Snížení vysílacího výkonu** – V případě velkého vytížení média by zařízení mohla dynamicky regulovat svůj vysílací výkon a tím omezit zásahy do komunikace vzdálenějších zařízení. Dochází tím ovšem k dalšímu snížení dosahu, který je již nyní značnou slabinou 802.11p. Ad-hoc síť bez možnosti centrální regulace také představuje komplikované prostředí pro detekci a smysluplnou koordinovanou regulaci obsazení kanálů.
- **Inteligentní směrování paketů DENM** – CAM zprávy vzhledem ke své opakovatelnosti představují většinu C2X komunikace, jedná se ale o single-hop komunikaci. DENM zprávy se v DSRC sítí ovšem přeposílají formou definovaného počtu skoků. Zde mohou vznikat problémy s náhlým přehlcením sítě, kdy více vozidel detekuje událost, na základě které bude odeslán DENM. Všechna vozidla zároveň začnou přeposílat jedno druhému a dalším tu samou zprávu, dokud není vyčerpán počet přeposlání. Tímto je médium zbytečně zahlceno redundantními zprávami, které OBU jednotky přijímají z mnoha míst,

filtrují a zahazují. Řešením tohoto problému by mohlo být použití multicast směrování na základě geolokace (např. neadresovat vozy, které se vyskytují v dosahu události) namísto obyčejného broadcastu. Vozy v dosahu události v době bezprostředně po jejím vzniku by si také mohly vyměnit informace o domluvě, kdo bude data přeposílat dál, takové řešení se ovšem jeví jako technicky komplikované.

- **Dynamické směrování signálu na prostor vozovky** – V současnosti se pro DSRC plánuje nasazení standardních všesměrových antén. Metoda směrování vyzářeného signálu (tzv. beamforming) na oblast vozovky, po které se vozidlo pohybuje, by uvolnila médium, které všesměrová anténa obsazuje v místech, kde jsou daná vysílaná data irelevantní. Může se jednat například o vedlejší silnici, na které je C2X komunikace omezena kvůli vyzařování vozidel z paralelně vedoucí dálnice. Vzhledem ke skutečnosti, že vozidla jsou omezena pohybem po silnicích, na kterých se nacházejí a komunikují pouze s ostatními vozidly či RSU na dané vozovce, nemá všesměrové vysílání a příjem žádný pozitivní význam. Nevýhodu dynamicky směrovaných antén představuje zvýšená vývojová i jednicová cena oproti anténě klasické, s kruhovou oblastí vyzařování. Touto problematikou se podrobně zabývá autor [19], jehož řešení je již předmětem návrhu patentu.

Jak je z diskuze nad navrhnutými opatřeními zjevné, každé má své zápory. Pro nápravu problému zahlcení média se tedy jeví jako optimální implementace všech zmíněných opatření v určité míře. V tomto ohledu je potřeba provést rozsáhlá měření různých kombinací vysílacích rychlostí, velikostí rámců s různými intervaly mezi vysíláním atd., jejichž výsledkem by měl být optimální poměr mezi uvolněním zatížených kanálů a zachováním bezpečnosti, která představuje hlavní motivaci k implementaci technologie.

Zahlcení pásem LTE

3.2.2	Zahlcení média	4	2	5	**40**

Zahlcení média také představuje problém u řešení C2X prostřednictvím sítě LTE, zde RPN ovšem nabylo hodnoty pouze 40 zejména z důvodu mnohem nižší předpokládané pravděpodobnosti výskytu takové události a její opakovatelnosti. Je to zapříčiněno

zejména architekturou sítě, kde je přidělování komunikačních kanálů řešeno centrálně, přičemž mnoho problémů se zahlcením vzniká právě z decentralizované podoby DSRC sítí.

Přesto situace v celulárních sítích není ideální, bezpečnostně relevantní a kritická komunikace by zde sdílela frekvenční spektrum se všemi ostatními uživateli mobilních sítí a již dnes se LTE potýká s nedostatkem spektra. Řešením je přidělení dalších frekvenčních pásem této celulární technologii a ji následujícím, což má ovšem negativní následky na technologie, kterými jsou tato pásma v současnosti obsazena. Vzhledem k počtu uživatelů těchto sítí a objemu dat po nich přenášených je také potřebné alokovat nějaké pásmo pouze pro C2C a C2I (případně C2P) komunikaci. Kandidátem pro alokaci tohoto pásma je například pásmo 450 MHz, které by mohly uvolnit rušící se datové CDMA sítě. Výhodou tohoto pásma je velký dosah, který je pro C2X nutný vzhledem k potřebě plošného pokrytí.

4.5.2 Kompromitace sítě

V této části jsou rozebrány návrhy možného omezení všech identifikovaných způsobů útoků na síť či narušení soukromí jejích uživatelů. Většinu typů útoků, mezi které patří vysílání falešných dat o dopravě (záměrné způsobení nehody, vytváření zelené vlny pro průjezd atd.), vystupování pod falešnou identitou či sledování pohybu uživatelů sítě, odstraňují již definované bezpečnostní prvky, především PKI. Stále ale existuje řada způsobů prolomení zabezpečení systému, které představují výraznou překážku pro nasazení C2X technologií do provozu.

PKI a certifikáty

2.1.2	Kompromitace identity žadatele o certifikáty	4	2	5	**40**

Jak již bylo zmíněno, PKI schéma, které má C2X DSRC používat, eliminuje většinu možností neoprávněného vysílání či odposlechu komunikace v C2X síti, jelikož každé vysílající OBU a RSU je ověřeno certifikační autoritou. Zde ovšem vzniká hlavní problém této bezpečnostní architektury – každý, kdo v síti komunikuje, je nucen spoléhat na důvěryhodnost dané CA. Jedinec uvnitř takové CA může přitom disponovat přístupem

k zneužitelným datům kompromitujícím identitu certifikovaných jednotek. Z tohoto důvodu je stěžejní, aby bylo zachováno specifikacím odpovídající rozdělení CA na PCA a LTCA, přičemž je důležité, aby byla každá autorita provozována jinou entitou. Pokud by došlo ke spojení těchto autorit či jejich administraci jediným provozovatelem, jak je často plánováno alespoň pro první náběh C2X (z důvodu nižších nákladů a komplexity), měl by takový provozovatel všechna potřebná data pro odhalení identity jakéhokoliv vozu pod ním certifikovaným. K udržení důvěryhodnosti CA by také přispěly pravidelné recertifikace kořenovými certifikačními autoritami spojené s audity, společně s možností provedení neplánovaných auditů.

Vozidla zapojena do PKI mohou přijít o svou anonymitu i analýzou samotného krátkodobého certifikátu, jeho obsahem jsou totiž například specifická síťová oprávnění – řešením je vytvoření malého množství skupin (RSU, běžné vozidlo, záchranné složky atd.) namísto užívání konkrétních práv pro každého účastníka, které mohou vést k jeho identifikaci.

Integrita a důvěrnost v LTE

3.1.1	Není zajištěna důvěrnost vůči provozovateli sítě	4	3	3	**36**
3.1.2	Není zajištěna integrita při komunikaci v síti	5	3	5	**75**

Jak již bylo dříve popsáno, celulární sítě LTE v současnosti nesplňují požadavky na zachování skryté identity (vůči provozovateli sítě) a především integritu dat v případě D2D komunikace, které v DSRC garantuje správná implementace PKI. Tudíž se otevírá možnost útočníkům realizovat útoky přehráním (pozdržení či pozdější zopakování odchycených validních dat), maskováním (předstírání cizí identity) a mnoho dalších. Jednoduchým řešením je adaptace bezpečnostních standardů DSRC z IEEE 1609.2, především právě PKI, které tyto problémy úspěšně řeší. Celý systém PKI by měl být ovšem provozován nezávisle na poskytovateli sítě, čímž by byla omezena i schopnost operátora členy C2X sítě sledovat.

Zneužití věrohodné jednotky

1.1.2	Používání certifikované jednotky mimo vozidlo či stanici, pro kterou je určena.	5	2	5	**50**

Implementované bezpečnostní metody nedovolují neautorizovaným zařízením podílet se na komunikaci, jedním ze způsobů útoku na síť tedy může být použití OBU či RSU, které je úspěšně certifikováno jeho vyjmutím a připojením k simulační platformě. Takovému útoku lze předejít implementací funkce ochrany komponent, která zablokuje veškerou funkcionalitu jednotky, pokud detekuje, že není připojena ke správné interní síti. Tento způsob znemožnění použití elektronické komponenty používají výrobci automobilů již dnes jako ochranu proti odcizení, například u systémů infotainment (znemožněním zvýšení hlasitosti), jeho účinnost je tedy praxí ověřena. Zároveň, protože systém již existuje, jeho přenesení na ITS jednotky nevyžaduje nákladný vývoj. Jedná se tedy o velmi účinné a nenákladné řešení tohoto jinak závažného problému.

Konkrétní chování ITS jednotky v případě připojení k neznámému rozhraní by mohlo například spočívat ve formátování perzistentní paměti, ve které jsou uloženy krátkodobé certifikáty a suspenzi další funkcionality či sebenahlášení certifikační autoritě (pokud je k dispozici připojení k internetové síti), která ji přidá na revokační seznam.

1.3.2	Poskytování falešných signálů OBU pro tvorbu C2X rámců	5	2	3	**30**

ITS jednotka nemusí být pro možnost zneužití odebrána ze svého definovaného stanoviště (vozu, semaforu atd.), simulátor CAN či automotive Ethernet rámců může být připojen přímo k interní síti vozu buďto prostřednictvím diagnostické zásuvky či bezdrátově. V takovém případě lze přinutit nedostatečně chráněnou ITS jednotku k vysílání manipulovaných zpráv s libovolnými parametry. Je tedy potřeba, aby byly všechny vstupy do interní sítě vozu chráněny proti neoprávněnému vniknutí, to znamená například umožnění diagnostiky vozidla pouze při online propojení se servery výrobce či implementaci robustních firewallů a whitelistů, které neumožní příjem jiných než definovaných zpráv na všech bezdrátových vstupech do interní sítě vozu. Možností je také implementace autentizace, důvěrnosti a integrity pro interní síť, které by zaručily, že

OBU přijme pouze autentická data z reálných jednotek ve voze. Šifrování v současnosti sítě vozů neaplikují, protože jsou zatím uzavřenými systémy pro komunikaci mezi řídícími jednotkami, bez vnější interakce. Sběrnice ve voze musí být ovšem především jednoduché a schopné předávat data v reálnému času s minimální odezvou, implementace bezpečnostních algoritmů by tedy mohla způsobit značná zpomalení a kompromitovat tak funkci ostatních ECU i samotné OBU, časově omezené při konstrukci zpráv. Zavedení tohoto opatření by tedy mohlo mít značné negativní důsledky a je doporučeno jej neaplikovat, jelikož samotné zabezpečení vstupů k těmto sběrnicím by mělo být dostatečnou prevencí neoprávněných zásahů.

1.2.1	Odesílání falešných pozičních dat OBU ke zpracování	5	2	5	**50**

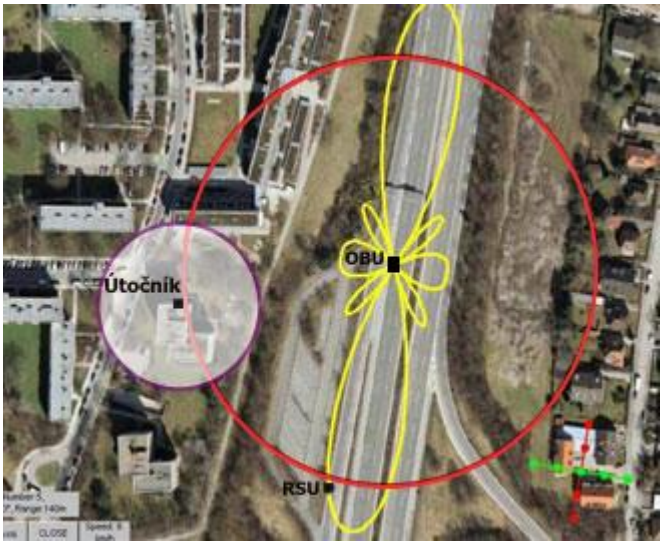
Obzvláštně nebezpečnou a náročně detekovatelnou formou manipulace s daty, které OBU přijímá, je vysílání falešných pozičních dat a zmatení GNSS přijímače (satelitní signál je na zemi velmi slabý a lze ho snadno překonat). Proti této formě útoku je potřeba zdokonalit metody detekce nepravého GNSS signálu na straně GNSS jednotky (porovnání směru příchodu signálu, anomálie v přijatém signálu atd.). Jelikož lze ovšem čekat, že pokročilé metody falšování signálu GNSS přijímač obelstí, mělo by OBU kontrolovat validitu přijatých dat, to ovšem přidává další výpočetní nároky a tudíž časovou náročnost při tvorbě každé zprávy, je tudíž opět potřeba zvolit kompromis mezi rychlostí algoritmu kontroly plauzibility a kvalitou ohodnocení daného signálu.

Cílené frekvenční rušení

2.3.4	Cílené frekvenční rušení	5	2	5	**50**

Cílené rušení frekvencí vysíláním šumu o vysokém výkonu představuje obzvláště v případě DSRC, kde při vyrušení všech sedmi kanálů nelze využít jiného pásma, formu útoku, proti které v současných standardech není žádná obrana. Proti útokům na fyzické úrovni se obecně brání problematicky, zároveň je takový útok velmi těžko odhalitelný, pokud útočník používá inteligentní reaktivní rušičku, která vysílá šum na dané frekvenci pouze ve chvílích, kdy se snaží vysílat ostatní. Přesto, že se jedná o lehce proveditelný

útok vyřazující potencionálně kritickou komunikaci v daném místě a jeho odhalitelnost v dané situaci může být náročná, RPN zde nenabývá neakceptovatelných hodnot. Je tomu tak z důvodu, že takový útok není příliš pravděpodobný, jelikož útočník jím nemůže nic získat (během rušení nelze odposlouchávat, ani posílat), kromě zabránění v komunikaci ostatním. Výskyt tohoto útoku lze tedy předpokládat velmi sporadicky, provedený zejména amatéry na malé ploše. Efektivní obranou by opět mohl být beamforming navrhnutý p. Stübingem v [19]. Lze totiž předpokládat, že takový útočník se nachází za krajnicí silnice. Tím, že antény vozu nebudou v tomto prostoru přijímat signál, rušivá frekvence nebude odchycena (viz obrázek 9).



Obrázek 8 - porovnání vyzařování antény s a bez užití tvarování signálu

Obecně

Univerzální obranou proti zde zmíněným způsobům zneužití autorizovaných jednotek mohou být vyspělé algoritmy detekce plauzibility zpráv společné s hlášením podezřelých odesílatelů certifikační autoritě. Ta může na základě počtu automatických nahlášení poté zneplatnit aktuální pseudonymy, v případě opakování LTCA provede revokaci dlouhodobého certifikátu vozu, který bude bez možnosti čerpat další pseudonymy definitivně vyřazen z provozu.

4.5.3 Ostatní poruchy

Frekvenční rušení

2.3.3	Frekvenční rušení	2	1	5	**10**

Frekvenční rušení (ne záměrné) bývá nejčastějším tématem při hodnocení problémů bezdrátových sítí, přesto v této analýze byl tento mód poruchy ohodnocen pouze RPN =

10, tudíž nízkou rizikovostí. Důvodem je využití pásma 5,9 GHz pro DSRC, po kterém nekomunikují žádné jiné technologie, k vzájemnému rušení tedy nedochází, přestože se přímo ve voze nachází velké množství jiných vysílajících radiofrekvenčních technologií. Jediný problém může představovat sousední pásmo 5,8 GHz, které v Evropě využívá CEN DSRC pro elektronickou kontrolu mýtného. Řešením interference je snížení vysílacího výkonu či krátkodobé odstavení C2C a C2I komunikace po dobu průjezdu mýtnou bránou – detekce CEN DSRC RSU je možná buďto na základě mapových podkladů (nevýhodou je nutnost aktualizace mapových podkladů při každé změně) či na základě přijmu signálu.

Současná bezproblémová situace se ovšem může změnit, jelikož Wi-Fi komunita ve Spojených státech amerických vyvíjí výrazný tlak na FCC, aby bylo pásmo 5,9 GHz sdíleno. Návrhy jsou vyklizení kanálu v případě detekce C2X vysílače (Cisco [52]) nebo omezení DSRC pásma na horních 30 MHz ze současných 75 MHz. Metoda „detect and avoid“ by při řádné implementaci teoreticky mohla zaručit koexistenci Wi-Fi a Car-to-X, riziko pozdního vyklizení pásma ovšem výrazně zvyšuje pravděpodobnost interference s teoreticky životně důležitými C2X pakety, v případě zavedení této metody by tedy došlo k navýšení faktoru pravděpodobnosti i následků (vysílání ve stejném, nikoliv pouze sousedním pásmu). Jednalo by se tedy o mnohem rizikovější stav, než za současné situace a přehodnocení z nízké rizikovosti na vysokou – z daného důvodu je problém zde rozebírán. Návrh druhý, omezení pásma, je z hlediska bezpečnosti provozu neakceptovatelný, jelikož již v současnosti představuje největší problém DSRC zahlcení pásma.

Přetížení ITS jednotky

1.1.3	Překročení výpočetní kapacity	5	3	5	**75**

Kromě zahlcení média může být závažným problémem ztrátovost paketů na straně přijímajících jednotek – dle výše provedeného odhadu by mohlo mezi vlastním vysíláním docházet k detekci až 2400 CAM paketů. Reálný počet přijímaných CAM by byl pravděpodobně nižší vzhledem k limitacím pásma a vzniklým kolizím, přesto je potřeba nastavení regulace příjmu těchto zpráv, jelikož OBU musí každý rámec vyhodnotit a dle

situace zpracovat (například převést do formátu rámců interní sítě vozu a odeslat). Navýšení výkonu a paralelizace procesů jednotky značně zvedá jednicové náklady, přitom není řešen problém přetížení vnitřní sítě velkým množstvím irelevantních rámců. Nabízí se tedy řešení vyvažováním zátěže založené na maximálním počtu verifikovaných zpráv za sekundu v závislosti na vzdálenosti odesílatele od příjemce a aktuálním výpočetním vytížení jednotky (přičemž zprávy překračující tyto meze budou bez verifikace zahozeny). Relevance a důležitost zpráv CAM klesá úměrně právě se vzdáleností, jedná se tedy o účinný způsob filtrace zpráv bez zvýšených nákladů na implementaci a kompromitace bezpečnosti. Toto opatření zároveň efektivně chrání proti případným DoS útokům.

Vytížení OBU	Vzdálenost od příjemce	Maximální frekvence zpracování zpráv
< 25 %	bez omezení	10 Hz
25 - 49 %	< 200 m	10 Hz
	≥ 200 m	5 Hz
50 - 74 %	< 100 m	10 Hz
	100 - 199 m	6 Hz
	≥ 200 m	3 Hz
75 - 89 %	< 100 m	10 Hz
	100 - 199 m	5 Hz
	200 - 299 m	3 Hz
	≥ 300	1 Hz
≥ 90%	< 100 m	8 Hz
	100 - 199 m	4 Hz
	200 - 299 m	2 Hz
	≥ 300	1 Hz

Tabulka 7 - Příklad hodnot pro navržený algoritmus vyvažování zátěže

Dosah vysílaného signálu u DSRC

2.3.2	Odeslaný rámec nedoručen vzdáleným příjemcům	3	4	5	**60**

Tuto zásadní limitaci decentralizované C2X komunikace lze na první pohled částečně řešit navýšením vysílacího výkonu, který nyní může dosahovat výkonu až 40 dBm na kanálu 184, to by ovšem dále umocnilo problém vzájemných interferencí a kolizí na obsazeném médiu. Možností tedy je vybudování husté sítě RSU podél komunikací, které budou DENM mezi sebou přeposílat a tím informaci šířit, pokud nedetekují jiné uzly

(OBU ve vozech) v dosahu. Takové řešení s sebou ovšem nese nutnost vybudování velmi nákladné infrastruktury vysílačů, která po většinu času nebude mít využití (události generující DENM nejsou časté).

Optimálním řešením je použití celulární datové sítě. Pokud dojde k události generující DENM a OBU nedetekuje žádnou další mobilní ITS jednotku v dosahu, dojde k odeslání zprávy prostřednictvím LTE. Takové řešení ovšem vytváří problém s adresací – pokud je vysílání hybridního charakteru a CAM jsou posílány lokálně, případná centrální správa, která DENM přijme, nemá informaci o lokaci vozidel, pro které je DENM relevantní. Vzniká tak potřeba komunikovat v určitých intervalech polohu a směr jízdy i prostřednictvím LTE, což vede k duplicitě vysílaných dat. Zároveň takové řešení vyžaduje plné uzpůsobení LTE sítí potřebám C2X. Jedná se tedy o argument pro využití LTE pro C2X komunikaci v plné míře. Jednodušším řešením je, že základnová stanice přijatý DENM rozešle všem v dané buňce, vzniklá množina příjemců je ovšem z hlediska relevance značně nepřesná.

Infrastruktura LTE sítí

3.2.1	Přetížení síťové infrastruktury	3	3	5	**45**
3.2.3	Ztráta spojení	5	5	3	**75**

Nízké pokrytí území signálem LTE či hrozba přetížení páteřního spojení sítě v současnosti představuje hlavní důvod pro upřednostnění DSRC komunikace. Vzhledem k růstovým tendencím mobilních sítí, stále se zvyšujícímu počtu jejich uživatelů a velkému nárůstu signálového pokrytí v posledních letech lze nicméně předpokládat, že infrastruktura bude v blízké budoucnosti značně rozšířena a modernizována, především s příchodem 4G a 5G sítí. Tato problémová situace, nyní vyhodnocena jako vysoce riziková až neakceptovatelná, tedy může být do pár let anulována.

3.2.4	Překročení maximální latence	3	2	5	**30**

Problém se zvýšenou latencí v LTE sítích nastává v případě jejich přetížení v důsledku mnoha připojených koncových zařízení, za zhoršených atmosférických podmínek

bránících signálu v cestě či způsobujících jeho rušení, ale také při komunikaci napříč více buňkami, kterou lze očekávat v případě C2X velmi často. Řešením je vývoj a implementace metod přímé komunikace mezi dvěma uzly účastnícími se C2X komunikace v síti LTE. Tím by došlo k přesměrování toku dat z vytížené páteřní infrastruktury celulární sítě přímo mezi účastníky provozu, kromě zajištění minimální latence shodující se s DSRC technologiemi je tak řešen i předešlý problém přetížení síťové infrastruktury. V tomto ohledu probíhá raná fáze standardizace LTE-V, vycházejícího z v současnosti zaváděného standardu LTE-D2D, zmíněného v kapitole tři. Přesto, že zatím o standardu LTE-V není nic známé, z výsledků analýzy je zjevné, že jeho vývoji je třeba věnovat značnou pozornost, mají-li být LTE sítě využívány pro C2X. LTE-V by také disponovalo výhodou oproti klasickému DSRC v centrálně řízeném přidělování komunikačních kanálů, které by zajišťovala síť, nebylo by tedy tak náchylné ke kolizím.

5 Závěr

Předmětem práce byla analýza potencionálních rizik bezdrátové radiofrekvenční komunikace mezi vozy a infrastrukturou Car-to-X s cílem nalézt možná opatření pro jejich minimalizaci. Zkoumána byla rizika týkající se lokální decentralizované komunikace založené na standardu IEEE 802.11p, centrálně řízené C2X komunikace využívající pro přenos dat celulární datové sítě 3GPP LTE a rizika obecně platná, nesouvisející s konkrétním způsobem přenosu dat. K této analýze byla použita metoda FMECA, prostřednictvím které bylo identifikováno celkem dvacet problematických stavů, přičemž pro každý z nich byla úspěšně navrhnuta opatření omezující jejich vliv na systém. Doporučená opatření byla dále rozebrána z hlediska jejich technické realizovatelnosti, nákladnosti na implementaci a případných úskalí, která přináší.

Při vyhodnocení analýzy bylo zjištěno, že hlavním problémem Car-to-X jsou v případě lokálního vysílání zahlcení alokovaného frekvenčního pásma 5,9 GHz, nicméně bylo navrženo celkem šest opatření, která tento problém mohou negovat. Patří mezi ně například regulace vysílacího výkonu, různorodé metody snížení času přenosu či inteligentní adresace DENM paketů. Přestože každá navržená metoda má svá úskalí, jejich vhodnou kombinací by mohlo být docíleno mnohem efektivnějšího využití 75 MHz širokého pásma. U centralizovaného přístupu pak byla identifikována rizika plynoucí z nízkého signálového pokrytí a dalších infrastrukturních nedostatků, především však nevyřešené otázky zabezpečení sítě a uchování anonymity jejích uživatelů, obzvláštně vůči provozovateli sítě – zde je doporučena především adaptace již existujících standardů pro DSRC.

Překvapivým zjištěním je fakt, že přestože pro lokální DSRC komunikaci byla za posledních deset let probíhající standardizace navržena velmi efektivní bezpečnostní opatření zajišťující autentičnost, integritu a důvěrnost přenášených dat, znemožňující většinu známých externích útoků, dosud nebylo řešeno riziko kompromitace systému důvěryhodným článkem zevnitř. Práce se tedy zabývá například riziky zneužití pozice věrohodné certifikační autority v rámci PKI schématu či zneužitím autorizovaného C2X vysílače pro generování fabulovaných zpráv, pro které též navrhuje realizovatelná

opatření, spočívající například v metodách zvýšení ochrany proti prolomení interní sítě vozu.

Přestože bylo v rámci analýzy nalezeno mnoho vysokých rizik spjatých s uvedením technologií Car-to-X do reálného provozu, implementací navržených opatření lze dosáhnout jejich snížení na akceptovatelnou úroveň, jež by umožnila plnohodnotné nasazení tohoto systému, který výrazně přispívá ke zvýšení bezpečnosti provozu a představuje nutnou podmínku pro vznik plně autonomních automobilů. Na práci lze dále navázat prototypovou implementací navržených metod či algoritmů a provedením experimentálních měření, na základě kterých lze ověřit validitu konkrétních opatření a upřesnit konkrétní parametry těchto metod.

Bibliografie

[1] **KOSCH, Timo; SCHROTH, Christoph; STRASSBERGER, Markus; BECHLER, Marc**. *Automotive Inter-networking. Chichester*, Spojené Království: A John Wiley & Sons, Ltd, Publication, 2012. ISBN: 978-0-470-74979-1.

[2] **U.S. Department of Transportation.** *CONNECTED VEHICLES: VEHICLE-TO-PEDESTRIAN COMMUNICATIONS.* Intelligent Transportation Systems Joint Program Office. [Online] [Citace: 15. únor 2017.] Dostupné z: http://www.its.dot.gov/factsheets/pdf/CV_V2Pcomms.pdf.

[3] **Siemens AG.** *Vehicle-to-X (V2X) communication technology*. 2015.

[4] **Transport for New South Wales.** *Cooperative Intelligent Transport Systems*. Transport for NSW. [Online] 16. leden 2016. [Citace: 18. únor 2017.] Dostupné z: http://roadsafety.transport.nsw.gov.au/research/roadsafetytechnology/cits/index.html.

[5] **FILIPPI, Alessio a spol.** *Why 802.11p beats LTE and 5G for V2x* . EE Times Europe Automotive. [Online] European Business Press SA, 21. duben 2016. [Citace: 20. únor 2017.] Dostupné z: http://www.automotive-eetimes.com/design-center/why-80211p-beats-lte-and-5g-v2x.

[6] **European Telecommunications Standards Institute.** *Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*. ETSI. [Online] 2012. [Citace: 21. únor 2017.] Dostupné z: http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.02.00_20/en_302663v010200a.pdf.

[7] **IEEE Vehicular Technology Society.** *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*. IEEE Standards Association. [Online] 2014. [Citace: 21. únor 2017.] Dostupné z: https://standards.ieee.org/findstds/standard/1609.0-2013.html

[8] **FEDERAL COMMUNICATIONS COMMISSION OFFICE OF ENGINEERING AND TECHNOLOGY POLICY AND RULES DIVISION.** *FCC ONLINE TABLE OF FREQUENCY ALLOCATIONS.* Federal Communications Commission. [Online] 31. srpen 2016. [Citace: 22. únor 2017.] Dostupné z: https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf.

[9] **Car 2 Car Commucation Consortium**. *Technical Approach.* Car 2 Car Commucation Consortium. [Online] 2016. [Citace: 21. únor 2017.] Dostupné z: https://www.car-2-car.org/ index.php?id=8.

[10] **RF Wireless World.** *Vehicular wireless communication tutorial | V2V vs V2i,C2C vs C2i.* RF Wireless World. [Online] [Citace: 25. únor 2017.] Dostupné z: http://www.rfwireless-world.com/Tutorials/vehicular-wireless-communication-tutorial.html.

[11] **SILL, Steve.** *DSRC: The Future of Safer Driving*. Intelligent Transportation Systems Joint Programm Office. [Online] U.S. Department of Transportation. [Citace: 25. únor 2017.] Dostupné z: http://www.its.dot.gov/factsheets/dsrc_factsheet.htm.

[12] **CAR 2 CAR Communication Consortium.** *Overview of the C2C-CC System* . C2C-CC System. [Online] 28. srpen 2007. [Citace: 26. únor 2017.] Dostupné z: http://elib.dlr.de/48380/1/C2C-CC_manifesto_v1.1.pdf.

[13] **SOMMER, Christoph; SEGATA, Michele; BLOESSL, Bastian.** *Vehicular Networks [C2X] Part 2: Car-to-X Networking Technology.* HEINZ NIXDORF INSTITUT. [Online] 2013. [Citace: 26. únor 2017.] Dostupné z: http://www.ccs-labs.org/teaching/c2x/2013s/08-tech.pdf.

[14] **European Telecommunications Standards Institute.** *ETSI TS 102 637-2 V1.2.1*. ETSI. [Online] březen 2011. [Citace: 26. únor 2017.] Dostupné z: http://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf.

[15] **ARANITI, Giuseppe a spol.** *LTE for Vehicular Networking: A Survey.* [Online] IEEE Communications Magazine, květen 2013. [Citace: 26. únor 2017.] Dostuúné z: https://www.researchgate.net/figure/236676802_fig4_Fig-4-CAMs-and-DENMs-delivery-in-IEEE-80211p-Messages-are-locally-broadcasted-through.

[16] **European Telecommunications Standards Institute.** *ETSI TS 102 637-3 V1.1.1.* [Online] ETSI, září 2010. [Citace: 26. únor 2017.] Dostuúné z: http://www.etsi.org/deliver/etsi_ts/102600_102699/10263703/01.01.01_60/ts_1026370 3v010101p.pdf.

[17] **SANTA, José a spol.** *Experimental evaluation of CAM and DENM messaging services in vehicular communications*. [Online] Transportation Research Part C Emerging Technologies Website, říjen 2014. [Citace: 26. únor 2017.] Dostupné z: https://www.researchgate.net/publication/263050012_Experimental_evaluation_of_CA M_and_DENM_messaging_services_in_vehicular_communications.

[18] **European Telecommunications Standards Institute.** *ETSI EN 302 637-2 V1.3.1.* ETSI. [Online] říjen 2014. [Citace: 26. únor 2017.] Dostupné z: http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.01_30/en_302637 02v010301v.pdf.

[19] **STÜBING, Hagen**. *Multilayered Security and Privacy Protection in Car-to-X Networks.* Darmstadt, Německo: Springer Vieweg, 2013. ISBN 978-3-658-02530-4.

[20] **European Commission, U.S. Department of Transportation.** *International Deployment of Cooperative Intelligent Transportation Systems - Bilateral Efforts of the European Commission and United States Department of Transportation.* European Commission. [Online] září 2012. [Citace: 28. únor 2017.] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/international-deployment-cooperative-intelligent-transportation-systems-bilateral-efforts.

[21] **European Telecommunications Standards Institute.** *ETSI TS 102 940 V1.1.1: ITS communications security architecture and security management*. ETSI. [Online] červen 2012. [Citace: 28. únor 2017.] Dostupné z: http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.01.01_60/ts_102940v010101p.pdf.

[22] **5G Americas.** *V2X Cellular Solutions*. 5G Americas. [Online] říjen 2016. [Citace: 28. únor 2017.] Dostupné z: http://www.5gamericas.org/files/2914/7769/1296/5GA_V2X_Report_FINAL_for_upload.pdf

[23] **Joint Research Centre.** *Cryptographic security mechanisms of the next generation digital tachograph system and future considerations.* European Commission. [Online] European Union, 2012. [Citace: 28. únor 2017.] Dostupné z: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC77933/lbna25663enn.pdf.

[24] **ARANITY, Giuseppe a spol.** *LTE for Vehicular Networking: A Survey*. [Online] IEEE Communications Magazine, květen 2013. [Citace: 1. březen 2017.] Dostupné z: https://www.researchgate.net/profile/Massimo_Condoluci/publication/236676802_LTE_for_Vehicular_Networking_A_Survey/links/0deec519bdc605949b000000/LTE-for-Vehicular-Networking-A-Survey.pdf.

[25] **EU-US ITS Task Force.** *Status of ITS Security Standards*. European Commission. [Online] 12. listopad 2012. [Citace: 3. březen 2017.] Dostupné z: ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1935.

[26] **IEEE Vehicular Technology Society.** *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*. IEEE. [Online] 26. duben 2013. [Citace: 2. březen 2017.] Dostupné z: http://ieeexplore.ieee.org/document/6509896/.

[27] **Car 2 Car Commucation Consortium.** *Mission & Objectives.* Car 2 Car Commucation Consortium. [Online] 2016. [Citace: 3. Březen 2017.] Dostupné z: https://www.car-2-car.org/index.php?id=8.

[28] **CAMP - VSC3 Consortium Proprietary.** *SAE J2735 DSRC Messag y e Dictionary.* Car 2 Car Communication Consorcium. [Online] 8. březen 2012. [Citace: 3. březen 2017.] Dostupné z: https://www.car-2-car.org/fileadmin/user_upload/OEM_Workshop_WOB/Message_Dictionary_Overview.pdf.

[29] **Ministry of Internal Affairs and Communications.** *Communications Policy and ITS Communications Policy and ITS in Japan.* MIC. [Online] 10. říjen 2007. [Citace: 3. březen 2017.] Dostupné z: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/071010_1.pdf.

[30] **Car 2 Car Communication Consorcium.** *Memorandum of Understanding for a harmonised Implementation and Deployment of cooperative ITS*. Car 2 Car Communication Consorcium. [Online] 27. červen 2011. [Citace: 4. březen 2017.] Dostupné z: https://www.car-2-car.org/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1488753129&hash=eae6139ea700aaa8e9dfdd76da4b25f97b5a0b26&file=fileadmin/downloads/PDFs/MoU_on_deployment-v40001.02_final.pdf

[31] **Car-2-Car Communication Consortium.** *Roadmaps beyond Day-1*. COoperative ITS DEployment Coordination Support. [Online] 7. březen 2016. [Citace: 3. březen 2017.] Dostupné z: http://www.codecs-project.eu/fileadmin/user_upload/pdfs/City_Pool_Workshop_1/CIMEC-CODECS_2016-03-3_Buburuzan.pdf.

[32] **BUBURUZAN, Teodor.** *ITS Standardization and Deployment as seen by a volume vehicle manufacurer*. ETSI. [Online] 2013. [Citace: 5. březen 2017.] Dostupné z: https://docbox.etsi.org/workshop/2013/201302_ITSWORKSHOP/S02_HOWDOSTANDARDSMATCHTHEPLANNEDDAYDEPLOYT/VOLKSWAGEN_Buburuzan.pdf.

[33] **SHI, Yi.** C-*ITS Status in China - To the 8th ETSI ITS Workshop*. ETSI. [Online] 8. březen 2015. [Citace: 5. březen 2017.] Dostupné z: https://docbox.etsi.org/Workshop/2016/201603_ITS_WORKSHOP/S01_CITS_STATUS_WORLD/CITS_CHINA_Huawei_YiShi.pdf.

[34] **HERNDON, Virginia**. *Audi announces the first vehicle to infrastructure (V2I) service - the new Traffic light information system.* AUDI USA. [Online] Audi of America, 15. srpen 2016. [Citace: 5. listopad 2016.] Dostupné z: https://www.audiusa.com/newsroom/news/press-releases/2016/08/audi-announces-first-vehicle-to-infrastructure-service.

[35] **NOVÁK, Pavel**. *Měření rušení ve Wi-Fi.* Praha, 2009. Bakalářská práce. České vysoké učení technické v Praze. Fakulta elektrotechnická. Katedra telekomunikační techniky.

[36] **CCM Benchmark Group.** *What is WiFi and How Does it Work?* CCM. [Online] březen 2017. [Citace: 21. březen 2017.] Dostupné z: http://ccm.net/faq/298-what-is-wifi-and-how-does-it-work.

[37] **National Instruments Corporation.** *WLAN - 802.11 a,b,g and n.* National Instruments. [Online] 23. září 2015. [Citace: 21. březen 2017.] Dostupné z: http://www.ni.com/tutorial/7131/en/.

[38] **POOLE, Ian.** *OFDM Orthogonal Frequency Division Multiplexing Tutorial*. Radio-electronics.com. [Online] Adrio Communications Ltd, 2017. [Citace: 25. březen 2017.] Dostupné z: http://www.radio-electronics.com/info/rf-technology-design/ofdm/ofdm-basics-tutorial.php.

[39] **POOLE, Ian**. *Wi-Fi/WLAN Channels, Frequencies, Bands & Bandwidths*. Radio-electronics.com. [Online] Adrio Communications Ltd. [Citace: 26. březen 2017.] Dostupné z: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php.

[40] **Tutorialspoint.** *Wi-Fi - Radio Modulation*. tutorialspoint. [Online] 2017. [Citace: 28. březen 2017.] Dostupné z: https://www.tutorialspoint.com/wi-fi/wifi_radio_modulation.htm.

[41] **STRANG, Thomas; RÖCKL, Matthias.** *Vehicle Networks V2X communication protocols*. STI Innsbruck. [Online] 2008. [Citace: 28. březen 2017.] Dostupné z: http://www.sti-innsbruck.at/sites/default/files/courses/fileadmin/documents/vn-ws0809/11-VN-WAVE.pdf.

[42] **SOMMERS, Christoph; DRESSLER, Falko.** *VEHICULAR NETWORKING.* Cambridge: Cambridge University Press, 2014. ISBN: 978-1107046719.

[43] **MIAO, Lusheng; DJOUANI, Karim a spol.** *A Survey of IEEE 802.11p MAC Protocol.* Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), September Edition, September 2011.

[44] **KENTA, Mori; OYUNCHIMEG, Shagdar a spol.** *Experimental Study on Channel Congestion using IEEE 802.11p Communication System.* HAL archives-ouvertres.fr. [Online] 11. březen 2013. [Citace: 29. březen 2017.] Dostupné z: https://hal.inria.fr/hal-00799218.

[45] **KHAIRNAR, Vaishali; KOTECHA, Ketan.** *Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment.* International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.2, March 2013.

[46] **VELSH, Ilya**. *Analýza uživatelské roviny mobilních sítí 4. generace*. Brno, 2014. Diplomová práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací

[47] **BUMBÁLEK, Z.** *Modulační techniky v moderních bezdrátových sítích*. Access Server. [Online] České vysoké učení technické v Praze, FEL , 8. únor 2010. [Citace: 3. duben 2017.] Dotupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2010020004zdroj.

[48] **VALIŠ, David.** *Analýza druhů, důsledků a kritičnosti poruch (FMEA-FMECA).* Technická univerzita Liberec, Fakulta mechatroniky, informatiky a mezioborových studií.

[49] **CARLSON, Carl S.** *Understanding and Applying the Fundamentals of FMEAs*. Annual RELIABILITY and MAINTAINABILITY Symposium. [Online] 2014. [Citace: 6. duben 2017.] Dostupné z: http://www.reliasoft.com/pubs/2014_RAMS_fundamentals_of_fmeas.pdf.

[50] **FISK, Margaret C.; BUTTERS, Jamie.** *Takata to Pay $1 Billion, Plead Guilty in U.S. Air Bag Probe*. Bloomberg. [Online] Bloomberg L. P., 13. leden 2017. [Citace: 11. duben 2017.] Dostupné z: https://www.bloomberg.com/news/articles/2017-01-13/takata-to-pay-1-billion-plead-guilty-in-u-s-air-bag-probe.

[51] **SHEPARDSON, David.** *U.S. judge approves $14.7 billion deal in VW diesel scandal.* Reuters. [Online] Reuters, 25. říjen 2016. [Citace: 30. duben 2017.] Dostupné z: http://www.reuters.com/article/us-volkswagen-emissions-idUSKCN12P22F.

[52] **National Public Safety Telecommunications Council.** *Parties Disagree on 5.9 GHz Sharing Issues*. NPSTC. [Online] [Citace: 22. duben 2017.] Dostupné z: https://blog.npstc.org/2016/07/11/parties-disagree-on-5-9-ghz-sharing-issues/.

Seznam příloh

Skupina	Funkce/ prvek	Pol.	Mód poruchy	Příčina poruchy	Následek na systém	Opatření	N	P	O	RPN
Obecné	ITS jednotka	1.1.1	Selhání elektroniky jednotky	Elektrický zkrat, výrobní vada, opotřebení	Kompletní výpadek funkce pro dané vozidlo nebo danou lokalitu (v případě RSU)	Všechny jednotky, včetně venkovních RSU, budou splňovat minimálně kvalitativní podmínky certifikace AEC pro elektronické komponenty v automotive.	5	1	1	**5**
		1.1.2	Používání certifikované jednotky mimo vozidlo či stanici, pro kterou je určena.	Jednotka je odebrána ze svého funkčního místa a připojena jinam	Zneužití jednotky pro neoprávněnou komunikaci v síti (vysílání fabulovaných zpráv)	Implementace ochrany komponent proti odcizení umožňující zablokování funkcí jednotky a smazání certifikátů, pokud bude připojena k jinému než k sobě registrovanému zařízení. Implementace pokročilých metod detekce plauzibility zpráv.	5	2	5	**50**
		1.1.3	Překročení výpočetní kapacity	Příliš mnoho přijímaných rámců - vysoký počet vysílajících zařízení nebo útok odepřením služby (DoS)	Jednotka je přehlcena a nedochází ke zpracování relevantních kritických rámců	Vyvažování zátěže založené na maximální frekvenci zpráv od specifického odesílatele v závislosti na vzdálenosti. Ignorování CAM rámců od určité vzdálenosti. Zvýšení počtu RSU jednotek a snížení jejich dosahu ve vytížených lokalitách (rozdělení zátěže).	5	3	5	**75**

	GNSS jednotka	1.2.1	Odesílání falešných pozičních dat OBU ke zpracování	Útočící vysílač generuje signál s polohovými daty o větší síle, než navigační satelity	OBU vysílá zprávy s falešnými pozičními daty a mystifikuje ostatní členy sítě	Metody detekce falešného GNSS signálu. Implementace pokročilých metod detekce plauzibility zpráv.	5	2	5	**50**
	Vnitřní síť vozu	1.3.1	Překročení maximálního času pro konstrukci zprávy	Nevyhovující síťová rozhraní ve voze či jednotka poskytující data	Rámce mohou být v době odeslání již nerelevantní	Minimalizace interní síťové komunikace implementací více funkčních prvků přímo do OBU (např. nerozrozdělení výpočetní a vysílací funkce do více jednotek, integrace interního GNSS modulu). Použití vyhrazeného CAN spojení pro C2X data ve voze.	2	2	3	**12**
		1.3.2	Poskytování falešných signálů OBU pro tvorbu C2X rámců	Napojení simulačního prostředí s možností simulace komunikace mezi řídícími jednotkami na vnitřní síť vozu a odesílání generovaných interních rámců OBU	ITS jednotka vysílá zprávy založené na padělaných vstupech - možnost útoku na síť a její uživatele (např. maskováním)	Robustní ochrana externích vstupů interní sítě - možnost spojení s interní sítí vozu a její diagnostikovatelnosti pouze během připojení ke kontrolním serverům výrobce. Ochrana všech bezdrátových vstupů do interní sítě včetně OBU (např. Firewall). Implementace autentizačních a důvěrnostních prvků v interní síti vozu.	5	2	3	**30**

	Interoperabilita	1.4.1	Vzájemná nekompatibilita C2X technologií	Mnoho nezávislých vývojových a normalizačních iniciativ, více technologických řešení, nedostatečná mezinárodní spolupráce	Vozy vyskytující se mimo svůj určený region nejsou schopny C2X komunikace	Spolupráce na interoperabilitě různých standardů (jako probíhá mezi USA a EU). Jednotnost používaného frekvenčního spektra. OBU jednotky schopné funkce s více standardy.	3	2	1	**6**
DSRC C2X	PKI zabezpečení	2.1.1	Nedojde k obnovení propadlých krátkodobých pseudonymových certifikátů	V intervalu potřebné obměny není dostupné spojení se servery certifikační autority	Vozidlo je vyřazeno z další Car-to-X komunikace	Více dostupných metod spojení s certifikační autoritou: - datové celulární spojení - WLAN (prostřednictvím Car2Home funkcionality) - IP spojení s RSU připojených k datovým sítím. Plánování včasných aktualizací.	4	4	1	**16**
		2.1.2	Kompromitace identity žadatele o certifikáty	Certifikát obsahuje příliš specifické informace umožňující odhadnout identitu žadatele. Únik dat o uživateli ze serverů certifikačních autorit.	Narušení soukromí uživatele, možnost sledování pohybu uživatele	Neomezovat množinu vozidel, které PCA certifikuje (např. výrobce, který provozuje PCA certifikující pouze vlastní vozy). Certifikáty nebudou obsahovat informace spojitelné s žadatelem. Striktní oddělení entit provozujících PCA a LTCA, udržování důvěryhodnosti všech CA pravidelnou recertifikací.	4	2	5	**40**

	Plné pokrytí okolí vozu signálem	2.2.1	Nepokrytí prostoru před vozem signálem	Útlum elektromagnetického signálu způsobený absorbcí a odrazem od skleněných střech vozů	Nemožnost vysílání a příjmu do a z prostoru nacházejícího se před přední částí vozu	Umístění druhé antény 5,9 GHz do přední části vozu - před skleněné prvky s tlumícími příměsemi	4	2	3	**24**
	Vysílání v rezervovaném pásmu 5,9 GHz	2.3.1	Zahlcení média	Příliš mnoho uzlů vysílajících v jedné lokalitě	Zahození paketů čekajících na odeslání - nedochází k výměně potencionálně kritických dat	Snížení velikosti CAM paketů. Snížení vysílacího výkonu. Použití vyšší přenosové rychlosti. Snížení frekvence odesílání CAM paketů. Implementace inteligentních směrovacích algoritmů pro multi-hop DENM rámce. Dynamické směrování signálu na prostor vozovky.	4	5	5	**100**
		2.3.2	Odeslaný rámec nedoručen vzdáleným příjemcům	Nízký vysílací dosah DSRC technologie	Nedoručení relevantních rámců příjemci	Zřízení husté sítě RSU podél komunikací nacházejících se ve vzájemném dosahu. Odeslání zprávy prostřednictvím celulární sítě, pokud nejsou detekovány jiné vysílající uzly v okolí.	3	4	5	**60**
		2.3.3	Frekvenční rušení	Sdílení spektra se standardní Wi-Fi. Jiná zařízení komunikující ve stejném či sousedícím frekvenčním pásmu	Vzájemné zarušení probíhající komunikace, některé signály jsou nečitelné	Udržení exkluzivity DSRC spektra pro Car-to-X komunikaci. Regulace výkonu při detekci vysílajícího zařízení v přilehlém pásmu.	2	1	5	**10**

		2.3.4	Cílené frekvenční rušení	Útok odepřením služby - vysílání náhodného šumu na stejných frekvencích, na kterých probíhá komunikace	Vyrušení veškeré komunikace na napadených frekvencích v dané lokalitě	Dynamické směrování signálu na prostor vozovky.	5	2	5	**50**
LTE C2X	Zabezpečení a ochrana soukromí	3.1.1	Není zajištěna důvěrnost vůči provozovateli sítě	Komunikace probíhá po síti monitorované jejím provozovatelem	Provozovatel sítě může sledovat pohyb konkrétních uživatelů.	Specifikace zabezpečení vyšší úrovně operujícího mimo doménu provozovatele sítě (převzetí PKI a jiných prvků bezpečnosti specifikovaných pro DSRC)	4	3	3	**36**
		3.1.2	Není zajištěna integrita při komunikaci v síti	Použití předem sdíleného symetrického klíče pro komunikaci v rámci skupiny koncových uzlů	Hrozba útoku přehráním, maskováním či jiné manipulace s daty "člověkem uprostřed"	Specifikace zabezpečení vyšší úrovně operujícího mimo doménu provozovatele sítě (převzetí PKI a jiných prvků bezpečnosti specifikovaných pro DSRC), včetně kontroly platnosti zprávy dle časové známky	5	3	5	**75**
	Vysílání v celulární síti	3.2.1	Přetížení síťové infrastruktury	Příliš mnoho vysílajících koncových zařízení	Nedoručení rámců - nedochází k výměně potencionálně kritických dat	Modernizace síťové infrastruktury (vybudování dodatečných základnových stanic, zvýšení kapacity páteřního připojení atd.).	3	3	5	**45**

		3.2.2	Zahlcení média	Příliš mnoho vysílajících koncových zařízení	Neodeslání nebo nedoručení rámců - nedochází k výměně potencionálně kritických dat	Uvolnění více frekvenčních pásem pro LTE a následné technologie. Rezervace speciálního pásma pouze pro bezpečnostně kritickou C2X komunikaci po vzoru DSRC	4	2	5	**40**
		3.2.3	Ztráta spojení	Vozidlo se nachází v oblasti mimo dosah základnové stanice LTE sítě.	Nemožnost vysílání a příjmu v síti	Rozšíření pokrytí celulárních datových sítích na veškeré oblasti se silniční infrastrukturou	5	5	3	**75**
		3.2.4	Překročení maximální latence	Síť je přetížena zpracováváním velkého množství komunikace. Nepříznivé atmosferické podmínky. Komunikace napříč více buňkami sítě - složité a zdlouhavé předávání.	Rámce jsou v době doručení již nerelevantní a dle časové známky prošlé, tudíž nepřijímány	Vysílání z globálního hlediska nepodstatných zpráv prostřednictvím D2D, bez zatěžování infrastruktury sítě.	3	2	5	**30**

Příloha B – Obsah přiloženého CD

Text bakalářské práce

– bakalarska_prace_2017_Dominik_Spiral.pdf

– bakalarske_prace_2017_Dominik_Spiral.docx

– kopie_zadani_bakalarska_prace_2017_Dominik_Spiral.pdf